ComConsult Research

Der Netzwerk Insider

Juli 2013

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Zonenarchitekturen: Notwendige Ordnungspolitik in Rechenzentrums- und Campus-Netzen

von Dr. Simon Hoff

Zonenarchitekturen dienen der sicherheitsorientierten Segmentierung von Netzen in Rechenzentrum (RZ) und Campus. Dabei kommen Techniken der logischen Netztrennung, der Kontrolle der Verkehrsflüsse an Netzübergängen sowie ggf. auch der Netzzugangskontrolle (Network Access Control, NAC) an Netzzugangspunkten zum Einsatz.

Solche Zonenarchitekturen verkomplizieren automatisch die Struktur der Netze und erhöhen den Betriebsaufwand erheblich. Ist ein solches Strukturierungsinstrument angesichts Virtualisierung und Cloud Computing überhaupt noch zeitgemäß? Interessanterweise ist die Antwort: Gerade dann! Sichere Virtualisierung erfordert beispielsweise eine sichere Trennung von produktivem und administrativem Netzverkehr, und Cloud Computing ist ohne mandantenfähige virtuelle Infrastrukturen nicht denkbar.

In diesem Artikel werden zunächst die grundlegenden Sicherheitsanforderungen diskutiert, die in der Praxis wesentlichen Architekturvarianten vorgestellt und typische Aspekte wie den Umgang mit Kurzschlüssen zwischen Sicherheitszonen betrachtet. Die Administration und Überwachung von Sicherheitszonen stellt dabei besondere Herausforderungen dar. Einführung und nachhaltige Umsetzung von einer Zonenarchitektur erfordern außerdem zwingend eine Anpassung und Erweiterung der IT-Prozesse.

weiter auf Seite 7

Zweitthema

Verkabelung am Arbeitsplatz: Alles wie gehabt?

von Dipl.-Ing. Hartmut Kell

Mit jeder in den letzten Jahren aufgetretenen technischen Innovation, insbesondere im Bereich der Arbeitsplatzverkabelung, erfolgte durch unterschiedlichste Interessengruppen eine Neudefinition der Nutzeranforderungen und sich daraus ableitender zwingender Orientierung hin zu besseren Kabel- und Steckerkomponenten. Selten entstand der Bedarf nach besseren Materialien beim Nutzer selbst, beispielsweise durch spürbare Einschränkungen der Nutzbarkeit von schlechten Verkabelungen. Prognostizierte man beispielsweise Anfang der 90er-Jahre einen kurzfristigen Bedarf nach „sehr hohen“ Datenraten am Arbeitsplatz (das waren „damals“ 100 Mbit/s), so entstand ein wirklicher Bedarf erst Mitte der 2000er, also 10-15 Jahre nach dem vorausgesagten Zeitraum der meisten Herstellerprognosen. Selbst heute, 20 Jahre später, kann festgestellt werden, dass in vielen Netzen erstaunlich viele Endgeräte noch mit 10 Mbit/s auskommen.

Die Tatsache, dass die meisten, auch älteren Tertiärverkabelungen eine Qualität besitzen, die eine Nutzbarkeit für die nächsten weiteren 5 bis 10 Jahre sicherstellen könnte liegt darin begründet, dass der Mehrpreis für eine Tertiärverkabelung mit einem höheren technischen Mehrwert in der Vergangenheit nur sehr gering war und somit die Entscheidung für bessere Verkabelungssysteme leicht zu treffen war.

weiter Seite 22

Geleit

SDN: Bedarf und offene Fragen

von Dr. Jürgen Suppan

ab Seite 2

Standpunkt

Jumbo Frames als „Nachbrenner“?

ab Seite 20

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2013

ab Seite 4

Neues Seminar

Seminar*plus* - IPv6 Grundlagen

ab Seite 21

Zum Geleit

SDN: Bedarf und offene Fragen

Das ComConsult-SDN-Forum gab einen guten Überblick über die aktuelle Situation, vor allem aber stellte es den gegebenen Bedarf den offenen Fragen gegenüber. Im folgenden soll ein kurzer Ausschnitt der vielen Diskussionspunkte gegeben werden, dies kann die Teilnahme an der Veranstaltung nicht ersetzen, aber wir werden das Thema zum RZ-Forum im November wieder aufgreifen.

Auch wenn SDN noch in den Kinderschuhen steckt, so gibt es durchaus einen greifbaren Bedarf. Darunter fallen u.a. folgende Anforderungen:

- Vereinfachter und preiswerterer Betrieb
- Selektive Umleitungen insbesondere in Sicherheits- und Analyse-Architekturen
- Dynamische Anpassungen an die vorhandene Bandbreite über starre QoS-Regeln hinaus
- Abstrahierung zur Trennung zwischen RZ-Architekturen und Netzwerken
- Steuerung von Netzwerk-Eigenschaften durch Anwendungen
- Zentrale Steuerung von Sicherheits- und Zonen-Architekturen

In den Diskussionen und auch Ankündigungen der Hersteller fallen dabei immer wieder die Bereiche Abstraktion und Sicherheits-Architekturen ins Auge.

Abstraktion ist eine wesentliche Voraussetzung für die weitere Automatisierung im Rechenzentrum insbesondere bei der Schaffung von automatischen Provisionierungen von Anwendungen und Diensten. Dabei geht es nicht nur um die Umsetzung neuer Service-Kataloge für die Anwender, sondern auch um mögliche Vereinfachungen und Optimierungen im 24/7-Operating. Automatisierung erfordert die Umsetzung einer ortsneutralen Kommunikation zwischen den verschiedenen Bestandteilen einer Applikation sowohl zum Zeitpunkt des Starts als auch während des Betriebs. Dies kann mit heutigen Netzwerk-Lösungen nicht geleistet werden. Die bisher zur Lösung dieses Problems geschaffenen Overlay oder Edge-Computing-Lösungen sind sicher geeignet das Problem zu lösen, schaffen aber in ihrer technischen Umsetzung neue Probleme gerade auch auf der Netzwerkseite.

Im Sicherheitsbereich geht es um eine verbesserte zentrale Kontrolle vieler verschiedener Sicherheits-Punkte zum Beispiel als Teil einer Zonenarchitektur, aber auch um die dynamische Reaktion auf kri-

tische Ereignisse. So fehlt in heutigen Lösungen die Möglichkeit eines dynamischen Re-Routings auf der Basis reiner Sicherheits-Erwägungen.

Ohne bei den genannten Bereichen in die Tiefe gehen zu wollen kann man klar feststellen, dass es einen messbaren und begründbaren Bedarf für SDN als Technologie gibt. Dies bedeutet allerdings nicht, dass alles bestehende durch SDN abgelöst werden wird. Aus heutiger Sicht schafft SDN ein weiteres, aber in seiner Ausprägung sehr wichtiges und effizientes Werkzeug, um den Netzwerk-Betrieb an immer komplexere Anforderungen anpassen zu können.

Betrachtet man die Produkt- und Technologie-Situation, dann muss SDN auch als mehrjährige Entwicklung gesehen werden, die in verschiedenen Phasen erfolgen wird. ComConsult Research hat auf dem SDN-Forum seine Prognose zur Marktentwicklung vorgestellt. (siehe Abbildung 1)

Die technische Bewertung des Bedarfs und der Fähigkeiten von SDN fällt überraschend positiv aus. Allerdings stehen dem durchaus kritische Fragen gegenüber, die in Summe das Potenzial haben, die gesamte Entwicklung auch zu blockieren. Beispiele für solche kritischen Fragen sind:

- Wie Hersteller-neutral und offen wird SDN?
- Wo kommen die Switches der Zukunft her, sind sie austauschbar?
- Sollen Applikationen wirklich Netzwerke steuern?
- Werden wir je SDN in Reinform erleben oder bleibt es bei hybriden Lösungen?
- Geht es auch ohne SDN?

Lassen Sie mich zu diesen Fragen einzeln Stellung beziehen:

Die zentrale Frage zur Zukunft der Netzwerke ist sicher die Hersteller-Neutralität. Die Fähigkeit, das jeweils beste Produkt zum Einsatz zu bringen und auch Produkte verschiedener Hersteller mischen zu können, ist für viele Umgebungen unverzichtbar und essentiell. In gewissen Grenzen ist das heute erfolgreich möglich. So wie die SDN-Entwicklung im Moment aber verläuft, muss durchaus die Frage gestellt werden, ob wir durch SDN nicht eine stärkere Hersteller-Bindung bekommen als bisher. Der Know-How-Bedarf und der Umfang der notwendigen Entwicklung

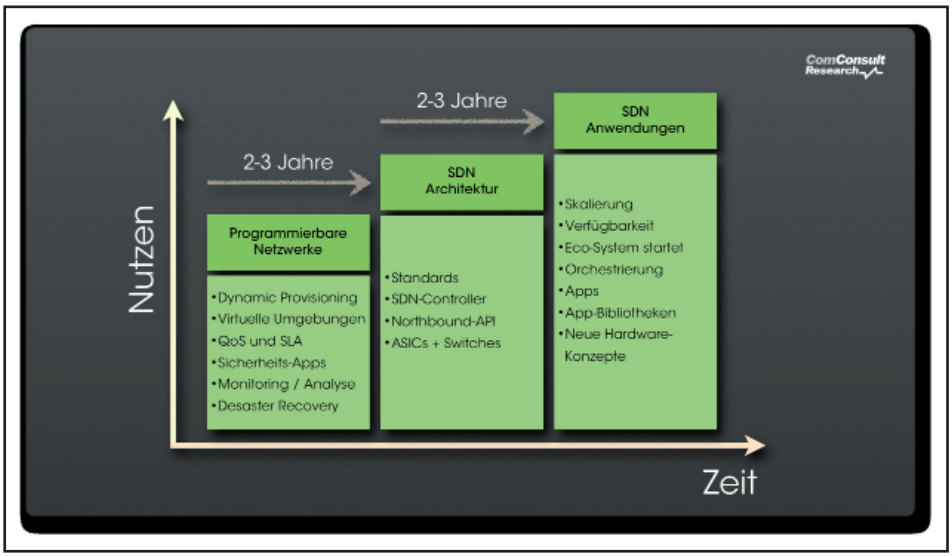


Abbildung 1: Prognose ComConsult Research

SDN: Bedarf und offene Fragen

kann zumindest kurz- und mittelfristig nur von sehr kapitalstarken Herstellern geleistet werden. Gleichzeitig ist der Einfluss der heutigen Hersteller auf die gesamte Entwicklung maximal, Open Daylight ist das herausragende Beispiel dafür.

In der reinen Lehre sind die SDN-Switches der Zukunft beliebig und austauschbar. Sie sollten sich in der Leistung und den physikalischen Schnittstellen unterscheiden, aber im Prinzip haben sie keine Eigenschaften mehr, die eine herstellerspezifische Lösung erfordert. Intel hat mit seinem Referenz-Modell für den Switch der Zukunft den Hut in den Ring geworfen und zielt genau in diese Richtung. Auch haben die ersten ASIC-Hersteller entsprechende ASICs für die nächsten zwei Jahre angekündigt. Trotzdem bleibt den Herstellern aber beliebig viel Spielraum, ihre Switches mit ihrem SDN-Controller eng zu bündeln. Hier kann man nur abwarten.

Eine der wirklich kritischen Fragen um programmierbare Netzwerke herum ist die Frage, ob es wirklich sein kann, dass Applikationen Netzwerke steuern. HP hat zusammen mit Microsoft eine Anwendung für den Lync-Server vorgestellt, bei der Lync sich seine Bandbreiten dynamisch selber abgreift. Man stelle sich vor, dass dies noch weitere Anwendungen machen. Wer gewinnt dann? Hier wird klar, dass zwischen Anwendungen und Netzwerken eine heute noch fehlende Schicht liegen muss, die wir als Orchestrierung bezeichnen. Anwendungen können ja ihre Wünsche ruhig äußern, aber die Bereitstellung der Ressourcen muss unter Berücksichtigung der Gesamtsituation erfolgen. Keine einzelne Applikation darf die Möglichkeit haben, das Netzwerk zu Ungunsten anderer Applikationen zu verbiegen. Diese Orchestration fehlt in der jetzigen SDN-Architektur ganz. Interessanterweise hat Cisco diese Funktion in seinem Programmiermodell für Netzwerke (was nicht SDN ist) eingeführt.

Hybride SDN-Lösungen sind keine Feigenblatt-Lösung. Wir brauchen sie zur stufenweisen Migration zu einer reinen SDN-Lösung. Sie haben in den meisten Fällen signifikante Performance-Einschränkungen und immer den Charakter einer Übergangs-Lösung. Aber sie gestatten bereits die Nutzung sehr interessanter und innerhalb der nächsten 6 Monate verfügbarer Mehrwert-Funktionen. Auf Dauer wird das reine SDN gebraucht, da jede andere Lösung nicht skalieren wird.

Geht es auch ohne SDN? Das ist eine wirklich gute und zentrale Frage. Die Antwort ist: bedingt ja. So können neue ASIC-Architekturen wie die des Fulcrum 6000 oder des Cisco-ASICs im 3850 viele Probleme vermeiden, auf die wir in der Vergangenheit gestoßen sind und die die Einführung von SDN notwendig gemacht haben (zum Beispiel die Unfähigkeit bestehender ASICs sich an neue Paketformate anzupassen, so dass für neue Verfahren neue Switches gekauft werden müssen). Aber diese ASICs sind beliebig, sie folgen keinem Standard. Von daher muss man die Frage stellen, ob sie wirklich eine solide Basis darstellen können. Für den Bereich Abstraktion gibt es bereits gute bestehende Alternativen auf der Basis von SPB. Aber zu SPB haben sich nur wenige Hersteller bekannt. Jedenfalls ist SPB besser als jedes Overlay-Gewurschtel.

Was bedeutet das nun?

Vereinfacht gesagt hat SDN viel Potenzial und wird mit Sicherheit kommen. Aber es gibt auch ernstzunehmende Zweifel und Bedenken an der Technologie. So wird es in vielen Bereichen Alternativen geben. Das macht SDN zu einem Baustein, aber nicht zur ultimativen Lösung. Zumindest nicht aus heutiger Sicht.

Die Empfehlung von ComConsult Research ist klar:

- Nehmen Sie SDN ernst und evaluieren Sie mögliche Vorteile
- Verlieren Sie die Risiken und Nachteile nicht aus dem Auge
- Starten Sie in den nächsten 6 Monaten einen Langzeit-Piloten und gewinnen Sie eigene Praxis-Erfahrungen
- Evaluieren Sie die neuen Produkte gerade aus dem Sicherheits-Bereich, so können kurzfristig Mehrwerte realisiert werden
- Akzeptieren Sie nur ein offenes SDN, akzeptieren Sie keine weitere Hersteller-Bindung
- Seien Sie sich über alternative Lösungen gerade im Umfeld von Automatisierungen und Sicherheits-Architekturen bewusst

Wir greifen das Thema für Sie in kritischer Form auf dem ComConsult Rechenzentrums Infrastruktur Redesign Forum 2013 in November auf und stellen dort unsere weitergehenden Analysen und Empfehlungen zu diesem Thema vor.

Ihr Dr. Jürgen Suppan

Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013
11.11. - 14.11.13 in Düsseldorf

Unsere Rechenzentren befinden sich in einer der größten Redesign-Phasen der letzten 20 Jahre. Nahezu alle Gestaltungs-Bausteine von den Servern, Speicher-Technologien, Netzwerken bis hin zu den Applikations-Applikationen sind im Umbruch. Gleichzeitig entstehen im direkten Umfeld durch eine Explosion mobiler Teilnehmer auf der einen und durch Cloud-Technologien auf der anderen Seite völlig neue Voraussetzungen. Diese gezielte Mischung aus Überblick, Analyse, Praxisberichten und Vertiefung macht diesen Kongress zu einem unverzichtbaren Termin für alle Planer, Betreiber und Führungskräfte.

Frühbucherphase bis zum 31.08.2013

Moderation: Dr. Behrooz Moayeri, Dr. Jürgen Suppan
Preise: € 2.290,-- (statt € 2.490,--)* - 4-tägige Veranstaltung
€ 1.890,-- (statt € 2.090,--)* - 3-tägige Veranstaltung
€ 790,-- (statt € 990,--)* - nur Intensiv-Tag
*rabattierte Preise gültig bis zum 31.08.2013 - dann reguläre Preise

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2013

23.09. - 24.09.13 in Euskirchen

Die ComConsult Akademie veranstaltet vom 23.09. bis 24.09.13 ihr "ComConsult IT-Sicherheits-Forum 2013" in Euskirchen.

Die Informationssicherheit muss stets flexibel und schnell auf neue Informationstechnologien reagieren. Idealerweise gestaltet sie die neue Technologie möglichst frühzeitig mit.

Wir werden uns bei dem diesjährigen IT-Sicherheits-Forum neben Best Practice in der Informationssicherheit daher mit folgenden aktuellen Themen befassen:

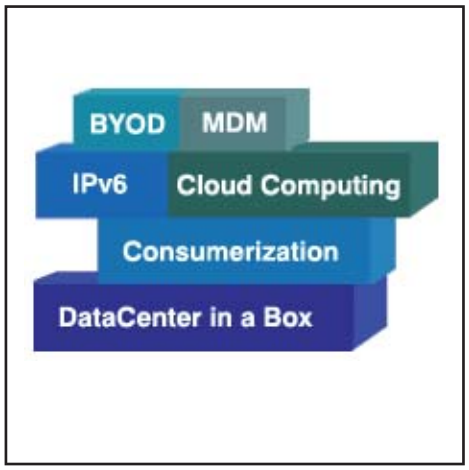
- Mit **Software Defined Networking (SDN)** zeichnet sich ein Paradigmenwechsel in Netzwerken und im Data Center ab, der sich massiv auf die Informationssicherheit auswirken wird.

- SDN ist ein weiterer Abstraktionslevel der Virtualisierung, bei dem wir nicht mehr nur virtuelle Server und Clients haben, auch die Netzwerkintelligenz wird virtualisiert. Dabei zeigen sich nicht nur Risiken, die frühzeitig berücksichtigt werden müssen, sondern auch höchst Interessante Möglichkeiten dieser Techniken für die Informationssicherheit ab. Ein provokatives Beispiel ist die theoretische Möglichkeit des Ersatzes einer traditionellen Firewall durch ein SDN-basiertes Regelwerk, das dynamisch auf Switches geladen und dort mit höchster Leistung abgearbeitet wird.

- **Cloud Computing** – anfänglich für den Enterprise-Bereich mehr belächelt als tatsächlich genutzt – ist inzwischen die strategische Ausrichtung für IT-Dienstleistungen geworden.

  Virtualisierungstechniken bilden die Basis für Cloud Computing. Das **Data Center in a Box** ist keine Vision mehr. Verschiedenste hochgradig dynamische komplett virtuelle IT-Infrastrukturen (d.h. Clients, Server, Netz und Storage), die gemeinsam auf einer physikalischen Hardware laufen, sind längst Realität.

  Sicherheitsmaßnahmen müssen sich daher stärker auf die Virtualisierungslösungen und die Anwendungen selbst konzentrieren.



- Plattformen für **Unified Communications (UC)** und für **Collaboration** wachsen zu **UCC** zusammen. Es bestehen hier erhebliche Anforderungen der Nutzer hinsichtlich eines flexiblen Datenaustauschs zwischen Unternehmen und Behörden. Die Absicherung von UCC muss dem gerecht werden.

- Im sogenannten **Internet of Things** erfassen Dinge (Things) – nicht Menschen wie im „Internet of Humans“ – Informationen, sind per IP vernetzt und stellen Informationen für andere Dinge oder Menschen zur Verfügung. Dahinter stecken natürlich unterschiedlichste Systeme und Anwendungen, bei denen Sensoren, Maschinen, Steuerungen, Fahrzeuge, etc. über IP untereinander und mit der Infrastruktur kommunizieren.

  Sicherheitsvorfälle im Internet of Things können erhebliche Folgen haben und der Schutz der „Things“ und ihrer Kommunikation ist daher von besonderer Bedeutung.

  Parallel zu diesen strategischen Entwicklungen haben wir in den letzten Monaten in einem gewissen Sinne eine Zäsur und vielleicht sogar das **Ende der Privatheit bzw. Vertraulichkeit** in der Informationstechnik erlebt: Es verging kaum noch eine Woche ohne das Bekanntwerden einer neuen qualitativ hochwertigen Spionage-Schadsoftware, ohne neue trickreiche Lauschattacken und die Aufdeckung zugehöriger Schwachstellen in IT-Systemen. Außerdem haben sich immer mehr Abgründe in der grenzenlosen Überwachung der Kommunikation im Internet (und nicht nur dort) aufgetan.

Diese Entwicklungen in der IT haben direkte Konsequenzen für die Informationssicherheit:

- Für den Nutzer einer virtuellen IT im Zeitalter des Cloud Computing muss sich die Informationssicherheit auf ihren Namen besinnen und Sicherheitsmaßnahmen müssen sich auf die Informationen selbst konzentrieren. Kernelemente sind nicht nur die Zusicherung von Vertraulichkeit und Authentizität durch Verschlüsselungstechniken sondern immer mehr auch die Nachvollziehbarkeit von Änderungen an Daten (Revisionsfähigkeit) und die Kontrolle von unerwünschtem Abfluss von Daten, d.h. letztendlich Klassifikation von Daten in Verbindung mit Data Loss Prevention.

- Die Absicherung von UCC muss verstärkt den Aspekt der Zusammenarbeit unterschiedlicher Unternehmen und Behörden berücksichtigen. Hier sind nicht nur Maßnahmen zur Absicherung von Voice und Video gefragt. Sicherheitsmaßnahmen müssen alle Kommunikationskanäle in UCC berücksichtigen, vom Chat, über Anwendungs- und Desktop-Sharing bis zum flexiblen Dokumentenaustausch.

- Wenn unterschiedliche, heterogene Gruppen von Nutzern und Geräten auf unterschiedlichem Sicherheitsniveau eine gemeinsame IT-Infrastruktur nutzen, muss diese in einem gewissen Umfang mandantenfähig sein. Dies erfordert stets die sichere Trennung der Informationen der Mandanten.

- Die traditionelle Methode der Informationssicherheit einer möglichst physikalischen Trennung auf Ebene des Netzes und der Endgeräte ist nicht mehr zeitgemäß. Virtualisierung erfordert ein Umdenken in Richtung logischer Trennung und insbesondere in Richtung kryptographischer Techniken.

Aktueller Kongress

- Zonenkonzepte in RZ und Campus sind zu einem normalen Gestaltungsinstrument geworden, stellen aber durch ihre Komplexität höchste Ansprüche an Planung und Betrieb. Schwerpunkte sind dabei die logische Trennung von Zonen in Virtualisierungsplattform, Netz und im Storage-Bereich.
- Wir benötigen sichere Identitäten in IP-Netzen und auf dieser Basis eine Netzzugangskontrolle mit dynamischer Berechtigung von Zugriffen
- Die klassischen Methoden und Prozesse der Informationssicherheit sind zu schwerfällig für eine IT, die maximale Mobilität für den Zugriff auf Information und für die Information selbst als Credo erhoben hat. Wir können nicht mehr für jede neue Anwendung aufwendige Sicherheitsbetrachtungen anstellen, wenn die Zeit zwischen Anforderungsanalyse und Produktivsetzung immer kürzer wird.

Aus diesen Gründen konzentriert sich das IT-Sicherheits-Forum 2013 auf folgende Themenbereiche:

- Konsequenzen von Software Defined Networking (SDN) auf Sicherheitsinfrastrukturen
- Sicherheit im Internet of Things – Konsequenzen der Verwendung von Standard-IT-Komponenten
- Das vernetzte Fahrzeug: Welche Möglichkeiten bereits heute bestehen, welche Gefährdungen hieraus resultieren und wie mit ihnen umgegangen werden kann
- Cloud Computing: Sicherer Nutzung von Clouds, Aufbau sicherer private Clouds und Anforderungen an sichere Public Clouds
- Konzentration auf Information: Verschlüsselung von Daten bei Transport und Speicherung, Datenklassifikation, Data Loss Prevention und Revisionsfähigkeit
- Sicherheit in UCC: Umgang mit dem Zielkonflikt zwischen möglichst flexibler Zusammenarbeit und der Absicherung der Daten
- Gefährdungen bei IPv6 und welche Maßnahmen heute möglich sind
- Sichere Identitäten in IP-Netzen
- Network Access Control (NAC) in der Praxis
- Mandantenfähigkeit und Zonenkonzepte in RZ und Campus: Netz- und Firewall-Architekturen, Server- und SAN/NAS-Anbindung
- Sicherer Betrieb von IT-Infrastrukturen: Authentisierung, Berechtigung, Protokollierung und Entkopplung der Kommunikation

Wie auch in den Vorjahren greift das IT-Sicherheits-Forum 2013 die aktuellsten Entwicklungen im Bereich der Informationssicherheit auf. Das Forum ist wie folgt strukturiert:

- Vorträge mit Top-Referenten und Erfahrungsberichten aus der Praxis
- Neueste Forschungsergebnisse der ComConsult für zukunftssichere Investitionen
- Begleitende Ausstellung in Kombination mit einem Vortragswettbewerb zur Präsentation der besten Projekte und Ideen in der Veranstaltung
- Happy Hour am ersten Tag

Das ComConsult IT-Sicherheits-Forum 2013 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2013. Sie ist für jeden Entscheider, IT-Sicherheitsbeauftragten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Frühbucherphase bis zum 31.07.2013

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IT-Sicherheits-Forum 2013

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2013

☐ vom 23.09. - 24.09.13 in Euskirchen
zum Preis € 1.690,--* netto

*gültig bis zum 31.07.13 - dann regulärer Preis € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

ComConsult-Study.tv

Cloud Spezial im Juli bei ComConsult-Study.tv

Cloud-Storage setzt sich immer mehr durch. Kaum noch ein Privatanwender, der es nicht nutzt. Sei es box.net, dropbox, Google Drive, die iCloud oder die der Telekom. Bei Unternehmen sieht es oft noch anders aus: sie wollen ihre Daten unter eigener Kontrolle haben und nicht in einer ominösen Cloud speichern. Doch kann man sich dem Trend verweigern? Cloud-Storage bietet viele Möglichkeiten aber auch Gefahren. In den drei Videos analysiert Dr. Suppan die Varianten. Abgerundet wird das Pakt durch den brandneuen Report „Speicher in der Cloud“ von ComConsult Research, der den Markt und die Möglichkeiten von Cloud-Speicherdiensten beleuchtet.

Standpunkt:
Cloud-Technologien für die RZ-Automatisierung?
Referent: **Dr. Jürgen Suppan**
Zeit: 00:34:08
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Cloud-Angebote basieren auf einem extremen Grad an Automatisierung. Neue Standards machen diese Technologien für alle Unternehmen zugänglich. Dr. Suppan analysiert welche Zukunfts-Bedeutung speziell OpenStack hat.

Cloud Storage in der Analyse
Referent: **Dr. Jürgen Suppan**
Zeit: 00:56:13
Einzelpreis: 39,00 € netto
Im Abo: kostenlos

Dr. Suppan stellt eine hochaktuelle Analyse von ComConsult Research zur Bedeutung von Cloud Storage für Behörden und Unternehmen vor.

Public und Private Clouds in der Analyse
Referent: **Dr. Jürgen Suppan**
Zeit: 00:55:59 gesamt
Einzelpreis: 59,00 € netto
Im Abo: kostenlos

Dr. Suppan analysiert die Vor- und Nachteile von Public und Private Clouds und leitet daraus Handlungsempfehlungen ab. Er zeigt wichtige Entwicklungen in der Cloud auf, stellt diesen aber auch die Risiken von Fehlentwicklungen gegenüber.

Speicher in der Cloud
Autor: **Dipl.-Math. Cornelius Höchel-Winter**
Veröffentlicht: Juli 2013 - ca. 50 Seiten
Kosten: € 249,-- netto

Die Integration externer Mitarbeiter und mobiler Endgeräte in die Unternehmensabläufe sowie die Einbindung und Anbindung externer Cloud-Dienste sind das zentrale Thema dieses Reports.

Das Bundle bestehend aus den drei Videos und dem Report kostet nur € 277,20*

*Dieses Angebot gilt nur im Juli 2013.- statt € 396,-- netto

Weitere Details finden Sie auf unserer Homepage unter www.comconsult-study.tv

Schwerpunktthema

Zonenarchitekturen: Notwendige Ordnungspolitik in Rechenzentrums- und Campus-Netzen

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Fortsetzung von Seite 1

1. Zonenarchitekturen als natürlicher Bestandteil der Enterprise Architecture

Manchmal muss es vielleicht erst zu Sicherheitsvorfällen kommen!

Erinnern wir uns kurz an typische, immer wieder auftretende Sicherheitsvorfälle:

- Kundendaten im internen Netz eines Providers waren bis zur Beseitigung einer Sicherheitslücke in einer Web-Applikation ungeschützt vom Internet aus abgreifbar.
- Durch den Anschluss eines Fremd-PCs eines Besuchers schaffte es ein Virus doch in das interne Netz und befiel PCs, die nicht mit einem (aktuellen) Virenschutz versehen werden konnten, da die PCs integriertes Element eines Geräts (z.B. in der Gebäudetechnik) waren, auf das die IT keinen direkten administrativen Zugriff hatte. Als Konsequenz fiel beispielsweise die Zutrittskontrolle zum und im Gebäude aus und Türen blieben verschlossen.
- Ein Angreifer konnte durch einen Trojaner auf einem Mitarbeiter-PC (oder einfach als Innentäter) einen Zugriff auf kritische Daten einer Institution erlangen und diese Daten über den Internet-Zugang der Institution nach draußen schmuggeln.

Diese Liste lässt sich wahrscheinlich beliebig fortsetzen. Solchen Vorfällen ist jedoch oft gemeinsam, dass von einem System oder einem Netz eingeschränkter Vertrauenswürdigkeit auf ein schützenswertes System bzw. Netz zugriffen wird. In vielen Fällen ist dann der Grund des Sicherheitsvorfalls in der unzureichenden Trennung von Systemen eingeschränkter Vertrauenswürdigkeit von den anderen IT-Systemen zu finden. Nicht selten ist dann eine Feststellung z.B. bei einem Sicherheits-Audit, dass das Netz aus dem Blickwinkel der Informationssicherheit nicht geeignet strukturiert ist.

Übertragung von Konzepten der Perimeter-Sicherheit auf das Intranet

Wir haben uns natürlich daran gewöhnt, dass wir unsere IT-Infrastruktur gegenüber externen, nicht oder eingeschränkt vertrauenswürdigen Netzen abschotten müssen. Wir haben dabei akzeptiert, dass eine Perimeter-Sicherheit komplexe Sicherheitskonstrukte erfordert, die aus ggf. mehrstufigen Firewall-Systemen und Demilitarized Zones (DMZs) an und zwischen den Firewall-Stufen zur Aufnahme von Gateways, Proxies, etc. besteht.

Die Vielfalt der unterschiedlichen Nutzergruppen und der Dienste und Anwendungen im Intranet und der damit verbundenen höchst heterogenen Sicherheitsanforderungen im Intranet erfordert nun, dass wir verstärkt Konzepte der Perimeter-Sicherheit auch zur Strukturierung des Intranet heranziehen müssen.

Notwendigkeit virtueller Tresore

Die Absicherung kritischer Daten vor unberechtigtem Zugriff (und damit verbunden vor Abfluss und Verlust) ist stets eines der wesentlichen Ziele der Informationssicherheit.

Für virtuelle Wertsachen, d.h. Daten mit hohem Schutzbedarf insbesondere hinsichtlich Vertraulichkeit und Integrität gilt das gleiche wie für physische Wertsachen: Sie kommen in einen Tresor, d.h. in

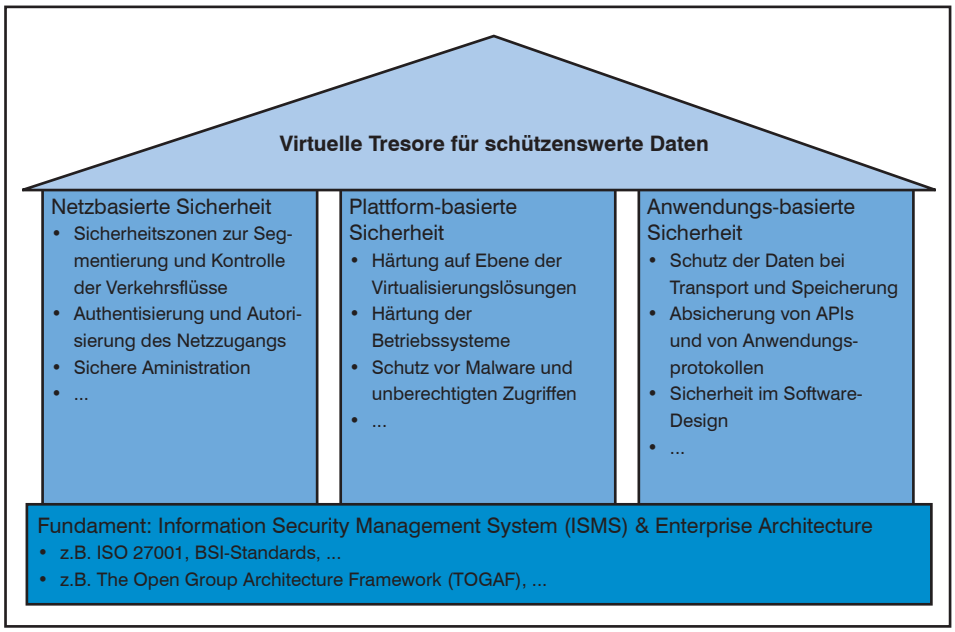


Abbildung 1: Fundament und tragende Säulen für den Aufbau von virtuellen Tresoren für schützenswerte Daten

einen Sicherheitsbereich. Ein solcher virtueller Tresor wird primär auf einer Kombination von drei Säulen der Informationssicherheit aufgebaut (siehe Abbildung 1):

- Netzbasierte Sicherheit
- Plattformbasierte Sicherheit
- Anwendungsbasierte Sicherheit

Dieser Artikel konzentriert sich auf die erste Säule der netzbasierten Sicherheit. Kernelemente sind dabei:

- Segmentierung eines Netzes in unterschiedliche Sicherheitszonen
- Kontrolle der Verkehrsflüsse zwischen Sicherheitszonen.
- Authentisierung und Autorisierung für einen entsprechenden Zugang zu einer Sicherheitszone
- Sichere Administration

Verankerung von Zonenarchitekturen in Standards zur Informationssicherheit

Die Forderung einer Zonierung ist auch in diversen Maßnahmenkatalogen zur Informationssicherheit entsprechend verankert. Schlägt man z.B. ISO 27001 (siehe [1]) im normativen Anhang A.11.4 „Zugangskontrolle für Netze“ auf, wird man über die Maßnahme A.11.4.5 „Trennung in Netzwerken“ stolpern: „Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzen getrennt gehalten werden.“

Diese kurze Formulierung hat es in sich, denn es wird klar und deutlich gemacht, dass auf Ebene des Netzes etwas geschehen muss. Diese Anforderung wird im Standard ISO 27002 (der als Best Practice für die Umsetzung von ISO 27001 zu verstehen ist) dann auch entsprechend konkretisiert. Die Umsetzung kann entweder mit den Mitteln einer Netztrennung und dem Einsatz einer Firewall am Netzübergang (jedoch grundsätzlich auch mit Access Control Lists, ACLs) oder durch kryptographische Techniken (z.B. VPN) erfolgen.

Maßnahme A.11.6.2 „Isolation sensibler Systeme“ von ISO 27001 fordert sogar verschärfend „Sensible Systeme müssen sich in einer dedizierten (isolierten) Umgebung befinden.“

Insgesamt kann also festgestellt werden, dass Zonenarchitekturen keinesfalls eine exotische Anforderung darstellen, sondern ein Standardelement moderner Unternehmensarchitekturen der IT sind.

2. Notwendige Bausteine einer Zonenarchitektur

Eine Zonenarchitektur muss zwingend einen modularen Bausteincharakter haben, denn es muss möglich sein, bei Bedarf flexibel im RZ neue Sicherheitszonen hinzufügen oder Server zu bestehenden Sicherheitszonen zuzuordnen. Aus dem Blickwinkel IT-Service muss es sogar möglich sein, für eine neue Sicherheitszone einen Bestellvorgang einzuleiten, der dann eine entsprechende Prozesskette in Bewegung setzt.

Terminologie: Ohne gemeinsame Sprache geht es nicht

Wie jede Architektur ist eine klare und konsequente Begriffsbildung für eine Zonenarchitektur entscheidend. Wie definiert sich der Begriff Sicherheitszone? Gibt es eine hierarchische Struktur oder eine logische Gruppierung von Sicherheitszonen an einem Standort einer Institution? Welche generellen Festlegungen zur Kommunikation zwischen Sicherheitszonen oder auf höheren Ebenen gibt es?

Folgende Festlegungen zu den grundlegenden Bausteinen einer Zonenarchitektur haben sich in der Praxis bewährt (was natürlich eine entsprechende andere, institutionsspezifische Anpassung keinesfalls ausschließt):

- Eine **netzbasierte Sicherheitszone** (im Folgenden kurz Sicherheitszone) ist ein IP-Netzwerk, das aus Sicherheitsgründen von anderen Netzen getrennt wird.
- Die Kommunikation in eine Sicherheitszone hinein oder aus einer Sicherheitszone heraus, wird durch Sicherheitsmaßnahmen kontrolliert. Hierzu werden die Sicherheitszonen durch **Sicherheitselemente** vernetzt.
- Sicherheitselemente werden je nach Anforderung ausgewählt. Beispiele sind Firewall oder Intrusion Prevention System (IPS).
- Innerhalb einer Sicherheitszone wird auf Ebene des Netzes die Kommunikation nicht eingeschränkt.
- Ein Sicherheitselement kann an mehrere Sicherheitszonen angebunden werden und eine Sicherheitszone kann ebenso mit mehreren Sicherheitselementen verbunden werden.

Auf diese Weise stellt sich das Intranet letztendlich als Netzwerk von Sicherheitszonen dar.

Festlegungen zur logischen und physischen Trennung

Wenn Sicherheitszonen durch IP-Netze gebildet werden, muss geregelt werden, unter welchen Rahmenbedingungen eine physische Trennung notwendig ist und wann eine logische Trennung auf Ebene von Netz, Servern und Clients erlaubt ist.

In Rechenzentren ist es beispielsweise heute inzwischen sogar üblich – sofern im Einzelfall keine spezifischen Sicherheitsanforderungen dem widersprechen – lediglich DMZ-Bereiche physisch zu trennen und ansonsten eine logische Trennung auf Ebene der Server und Netze zu gestatten. Dies erfordert natürlich eine entsprechende Absicherung von Netz und Virtualisierungsplattform. Ähnlich geht man auch in Campus-Bereichen vor.

Für eine logische Trennung in Netzen kommen beispielsweise auf Layer 2 Virtual LAN (VLAN) in Frage und oberhalb von Layer 2 sind Multiprotocol Label Switching (MPLS) sowie Virtual Routing and Forwarding (VRF) zu nennen. Auf Ebene der Endgeräte sind Server-Virtualisierung und Virtual Desktop Infrastructure (VDI) relevante Techniken.

Netztechnischer Aufbau einer Sicherheitszone

Im einfachsten Fall besteht eine Sicherheitszone aus einem einzelnen VLAN. Eine Firewall, die als Sicherheitselement an die Sicherheitszone angeschlossen ist, würde dann als Default Gateway für die Endgeräte in der Sicherheitszone dienen. Wenn eine Sicherheitszone aus mehreren VLANs, d.h. IP-Subnetzen, besteht, kann mit VRF gearbeitet werden (siehe Abbildung 2).

Bei standortübergreifenden Sicherheitszonen können die Sicherheitszonen im WAN mit MPLS-VPNs oder bei Carrier Ethernet letztendlich wieder per VLANs getrennt werden.

Die Anschaltung von Sicherheitselementen zur Kontrolle der Kommunikation zwischen den Sicherheitszonen erfolgt dann redundant an zentraler Stelle z.B. an Core Switches im Data Center.

Bei Firewalls ist dabei festzulegen, ob mit statischem Routing oder einem dynamischen Routing-Protokoll wie OSPF gearbeitet wird. In letzterem Fall würde OSPF dann auch das Redundanzverfahren bilden. Während OSPF bei Firewalls am Perimeter eher unüblich ist, kann OSPF für eine interne Firewall in jedem Fall in Betracht gezogen werden, sofern im LAN mit OSPF gearbeitet wird, um eine Einheitlichkeit, eine einfachere Konfiguration und eine Active-Active-Konfiguration der Firewalls zu erreichen. Andernfalls kann – wie im Perimeter-Bereich üblich – mit den Mitteln einer First-Hop-Redundanz per VRRP (oder einem vergleichbaren Verfahren) eine Active-Passive-Firewall-Redundanz geschaffen werden.

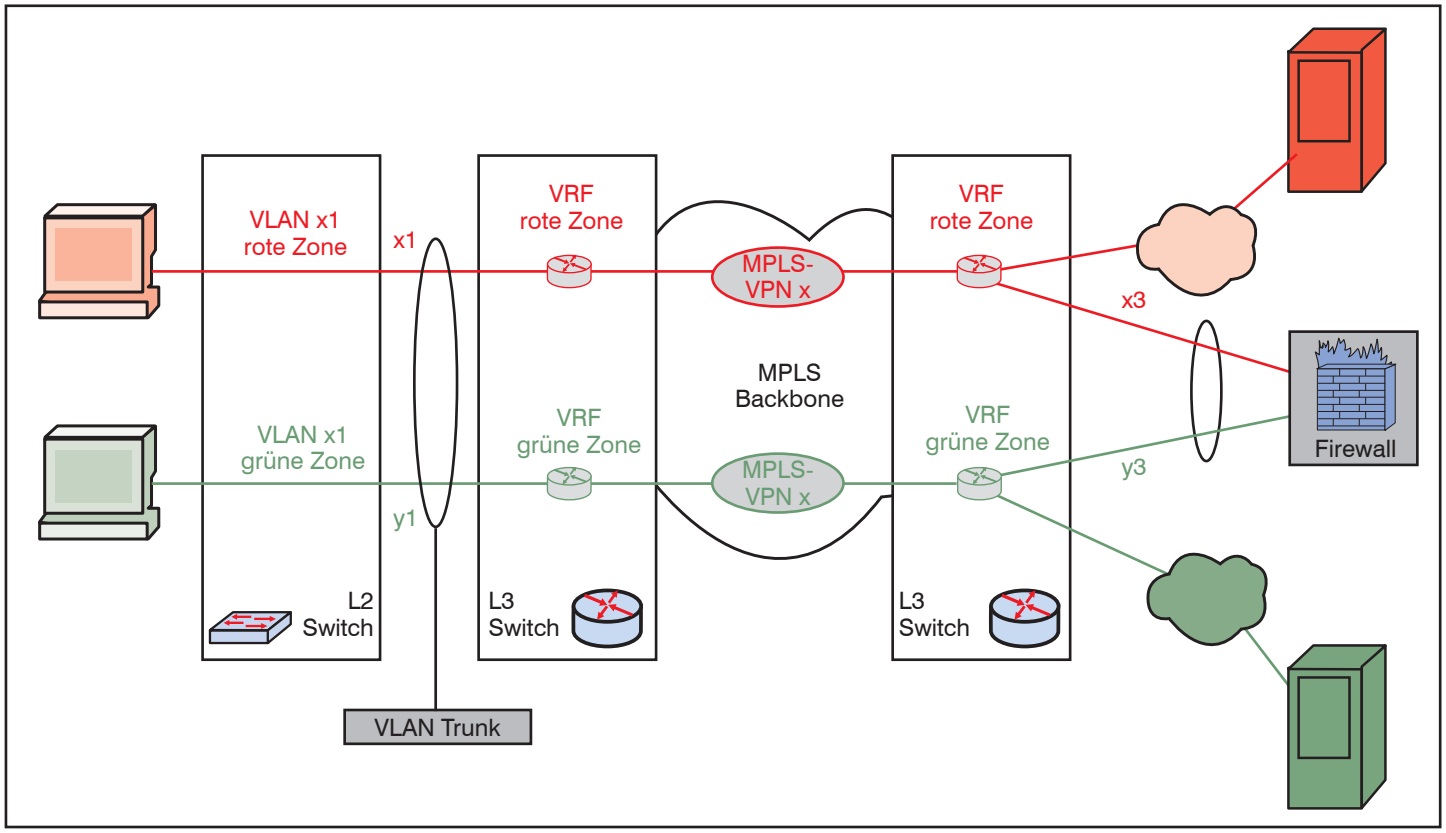


Abbildung 2: Beispiel einer Trennung von Sicherheitszonen

Aufbau bzw. Unterstützung von netzbasierten Sicherheitszonen durch kryptographische Techniken

Bei netzbasierten Sicherheitszonen kommen kryptographische Techniken wie IPsec primär zur Kopplung von Netzen über nicht oder eingeschränkt vertrauenswürde Bereiche in Frage (Site-to-Site VPN).

Es gibt allerdings eine Technik, die für die Absicherung der Kommunikation auf Layer 2 entwickelt worden ist, und die sich sehr gut dafür eignet, mandantenfähige Netze mit kryptographischen Techniken (und damit Sicherheitszonen im oben beschriebenen Sinn) zu realisieren: IEEE 802.11AE MAC Security (kurz: MACsec).

MACsec ergänzt das MAC-Layer der Netzelemente eines LAN um eine Hop-by-Hop-Absicherung, die Daten-Vertraulichkeit, -Integrität, -Authentisierung für die verbindungslose Kommunikation in einem LAN schafft (siehe [2]). MACsec erweitert hierzu das Frame-Format auf Layer 2 um ein Feld für Kontrollinformationen und um eine kryptographische Prüfsumme zur Integritätsprüfung und Authentisierung der Daten. Eine Verschlüsselung ist dabei optional. Die Prüfsumme geht sowohl über die Nutzdaten als auch über die MAC-Adressen und die MACsec-Kontroll-

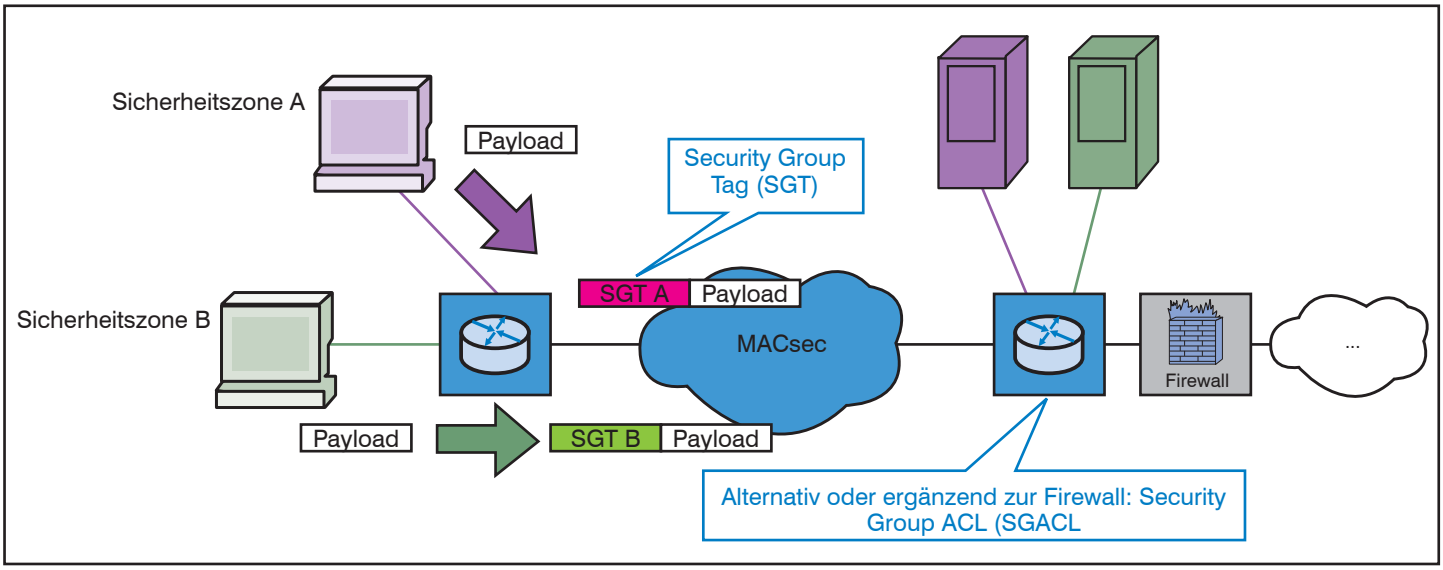


Abbildung 3: Beispiel für den Aufbau von Sicherheitszonen mit Cisco TrustSec

daten. Hierdurch werden insbesondere MAC-Spoofing-Attacken in LAN und Carrier Ethernet wirkungslos.

Im Feld für die Kontrollinformationen kann auch die Zugehörigkeit eines Pakets zu einer Gruppe bzw. einer Sicherheitszone geschützt gegen Manipulationen und Spoofing kodiert werden. Auf diese Weise können auf einer gemeinsamen Layer-2-Infrastruktur unterschiedliche Sicherheitszonen sicher voneinander getrennt werden.

Bisher hat allerdings nur der Hersteller Cisco diese Technik implementiert (Cisco TrustSec), unterstützt diese Technik jedoch nicht in allen Switches. Es ist jedoch grundsätzlich trotzdem möglich sowohl im RZ als auch in der Fläche auf dem Campus eine durchgängige Sicherheit und Mandantenfähigkeit mit TrustSec zu schaffen (siehe auch Abbildung 3). In der Praxis wird diese Möglichkeit derzeit noch recht selten verwendet.

Regelung für den Umgang mit Bereichen mit hohem Schutzbedarf

Wenn auf Virtualisierungs-Hosts VMs mit hohem Schutzbedarf hinsichtlich Vertraulichkeit, Integrität oder Verfügbarkeit betrieben werden, müssen neben Standardmaßnahmen zusätzliche Sicherheitsmaßnahmen ergriffen werden, um dem hohen Schutzbedarf gerecht zu werden. Dies ist insbesondere der Fall, wenn die VMs auf einem Virtualisierungs-Host ein signifikant unterschiedliches Sicherheitsniveau haben.

In der Praxis hat sich hier folgende Vorgehensweise bewährt:

1. **Absicherung der Virtualisierungslösung:** Basis ist neben der allgemeinen Schutzmaßnahmen für Server die Umsetzung der anwendbaren Maßnahmen des Grundschutzbausteins B 3.304 „Virtualisierung“ der BSI IT-Grundschutz-Kataloge (siehe [4]). Außerdem sind die entsprechenden herstellerspezifischen Standardmaßnahmen umzusetzen. Dies entspricht beispielsweise bei VMware dem Profile 3 des vSphere 5.1 Security Hardening Guide (siehe [5]).

   Um simultan Ressourcen für unterschiedliche Sicherheitszonen zur Verfügung zu stellen, muss die Virtualisierungslösung besonders gut gehärtet werden. Beispielsweise sollte für VMware bei einem hohen Schutzbedarf zusätzlich die Umsetzung des Maßnahmenkatalogs gemäß Profile 2 sowie im Hinblick auf Betriebstauglichkeit ausgewählter Maßnahmen des Profile 1 des vSphere 5.1 Security Hardening Guide (siehe [5]) erfolgen.

2. **VM-Normierung:** Wesentliches Element einer praktikablen sicheren Server-Virtualisierung ist die Normierung von virtuellen Servern. Dies beinhaltet zunächst Konfigurationsvorgaben an das Betriebssystem auf den virtuellen Servern sowie die Festlegung der Anwendungsbereiche und der Dienste.

3. **VM-Maßnahmenbündel:** Für jeden auf die beschriebene Weise normierten virtuellen Server wird ein Standardmaßnahmenbündel für den normalen Schutzbedarf (Mindesthärtung) sowie bei Bedarf ein hierauf aufbauendes erweitertes Maßnahmenbündel für den erhöhten Schutzbedarf festgelegt. Die wesentlichen Vorgaben werden dann als Konfigurationsrichtlinie für jedes Gastbetriebssystem festgelegt.

Eine ähnliche Vorgehensweise gilt auch für die Absicherung der Kommunikation im Netz. Hier ist insbesondere die Absicherung standortübergreifender Sicherheitszonen wichtig. Bei einem hohen Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität muss die Kommunikation über WAN- oder auch Standleitungsstrecken außerhalb des geschützten LAN möglichst verschlüsselt werden. Neben IPsec kommen hier MACsec und proprietäre Verschlüsselungslösungen („Kryptoboxen“) in Frage.

Kontrolle der Kommunikation zwischen Sicherheitszonen

Je nach Sicherheitszone sind unterschiedliche Anforderungen der Kontrolle der Kommunikation zu berücksichtigen.

Einerseits können besonders schützenswerte Endgeräte in einer Sicherheitszone vor unkontrollierten Zugriffen aus der sonstigen IT-Infrastruktur abgeschottet werden („Trusted Zone“). Dann dient ein Sicherheitselement an der Grenze zur Sicherheitszone primär dem Schutz der Sicherheitszone. Andererseits kann eine Sicherheitszone auch zum Schutz der weiteren Infrastruktur vor Endgeräten in der Sicherheitszone dienen („Untrusted Zone“).

Es gibt durchaus Situationen, in denen beide Aspekte für eine Sicherheitszone Anwendung finden. Ein Beispiel kann eine Sicherheitszone „Produktion“ sein, welche die IT für die industrielle Fertigung an einem Werksstandort eines Unternehmens aufnimmt. Eine solche Zone muss vor unberechtigten Zugriffen von außen besonders geschützt werden, da ein Ausfall der Produktion sofort einen erheblichen finanziellen Schaden verursacht. Umgekehrt findet man in Produktionsbereichen meist eine ausgesprochen heterogene Endgerätelandschaft, d.h. unterschiedlichste Betriebssysteme und insbesondere Altlasten ohne aktuelle Patches und Virenschutz. Außerdem werden meist diverse Systeme von Fremdfirmen lokal und remote betrieben. Daher hat die restliche IT-Infrastruktur auch ein vitales Interesse an einem Schutz vor der Produktion.

Als Sicherheitselement wird man in vielen Fällen ein zentrales, entsprechend leistungsfähiges und hochverfügbares Firewall-Systemen verwenden (im Folgenden auch als Data Center Firewall bezeichnet), das oft um Intrusion-Prevention-Funktionen ergänzt wird.

Die dabei zu verwaltenden Regelwerke können eine erhebliche Komplexität annehmen, da im Gegensatz zum Einsatz am Perimeter hier die Firewall internen LAN- und WAN-Verkehr filtern muss, d.h. mit dem gesamten im Intranet verwendeten IP-Protokollapparat zurechtkommen muss. Dies beinhaltet möglicherweise neben der Filterung von Protokollen, die dynamisch Ports aushandeln (z.B. RTP), auch die Erkennung von Sitzungen, die auf Basis von UDP aufgebaut werden (z.B. Authentisierungen via RADIUS).

Um eine bessere und einfachere Kontrolle über die Kommunikation zu erlangen, kann der Einsatz einer Next Generation Firewall (NGFW) in Betracht gezogen werden. Eine NGFW ermöglicht dabei zusätzlich identitätsbasierte Regeln auf Ebene der Anwendungen (siehe [6]). Zwar haben praktisch alle Hersteller von Enterprise Firewalls NGFW-Funktionen im Portfolio, die genannten Funktionen müssen jedoch ausgiebig getestet werden. Beispielsweise erfordert die Zuordnung von IP-Paketen zu Identitäten ggf. eine trickreiche Anbindung an Verzeichnisdienste, wie Active Directory.

Da bei der Filterung der Kommunikation zwischen Sicherheitszonen oft nicht nur Client-Server-Verkehr, sondern auch Server-Server-Verkehr gefiltert werden muss, ist nicht nur die Gesamtdurchsatzleistung einer Firewall bzw. eines IPS entscheidend. Von besonderer Wichtigkeit ist auch die Leistung pro Flow bzw. pro Session. Dies muss bei Hersteller-Auswahl und Dimensionierung zwingend berücksichtigt werden, will man keine Katastrophe bei Produktivsetzung des Firewall-Systems riskieren.

Bei der Filterung der Kommunikation an den Netzübergängen ist die Verwendung verschlüsselter Protokolle zu beachten. Wenn es gewünscht ist, dass die Filterkomponenten (z.B. ein IPS) den ver-

schlüsselten Verkehr analysieren, muss das Firewall-System um Verschlüsselungsendpunkte ergänzt werden, d.h. um entsprechende Proxies.

Insgesamt entsteht hier ein im Regelfall durchaus komplexes System.

Netzzugangskontrolle

An Sicherheitszonen im RZ werden meist nur Server angeschlossen. Diese Server befinden sich im RZ und daher in einem besonders geschützten und mit höchster Sorgfalt betriebenen Bereich. Es ist daher vielleicht nicht besonders wahrscheinlich, dass ein Server versehentlich oder mit Absicht an eine Sicherheitszone angeschlossen wird, zu der der Server nicht gehört.

In Campus-Bereichen ist die Situation meist anders.

Nehmen wir an, ein Client wird an einen aktivierten Netzwerk-Port angeschlossen, der einer Sicherheitszone zugeordnet ist. Dann ist ein Mechanismus wünschenswert, der an dem Port prüfen kann, ob das Endgerät tatsächlich auch zu dieser Sicherheitszone gehört. Nur wenn die Prüfung positiv ausfällt, sollte der gewünschte Zugang zur Sicherheitszone gewährt werden. Andernfalls sollte der Zugang abgewiesen oder nur ein (erheblich) eingeschränkter Zugang gewährt werden. Diese Authentisierung (d.h. Prüfung der Identität des Endgeräts bzw. des Nutzers des Endgeräts) sollte natürlich verlässlich sein, d.h. mit kryptographischen Mitteln erfolgen.

Analog könnte man fordern, dass für einen Client, der an einem Netzwerk-Port angeschlossen wird, im Rahmen der Authentisierung festgestellt wird, zu welcher Sicherheitszone das Gerät gehört, und nach erfolgreicher Authentisierung wird der Port dynamisch einem VLAN zugewiesen, das in das entsprechende Mandantennetz führt. Alternativ könnte hier auch mit ACLs gearbeitet werden, die am Netzwerk-Port dynamisch aktiviert werden.

Die Implementierung einer solchen Netzzugangskontrolle (Network Access Control, NAC) basiert meist auf dem Standard IEEE 802.1X (siehe [3]) in Kombination mit einer RADIUS-basierten MAC-Adress-Authentisierung und ggf. unter Nutzung eines sogenannten Captive Portal zur Browser-basierten Authentisierung z.B. von Gästen. In manchen Fällen kommen auch proprietäre NAC-Lösungen zum Einsatz.

Generell gilt jedoch, dass im kabelbasierten LAN NAC-Konzepte und deren Umsetzung sehr komplex und aufwendig sind (insbesondere im Vergleich zu WLAN).

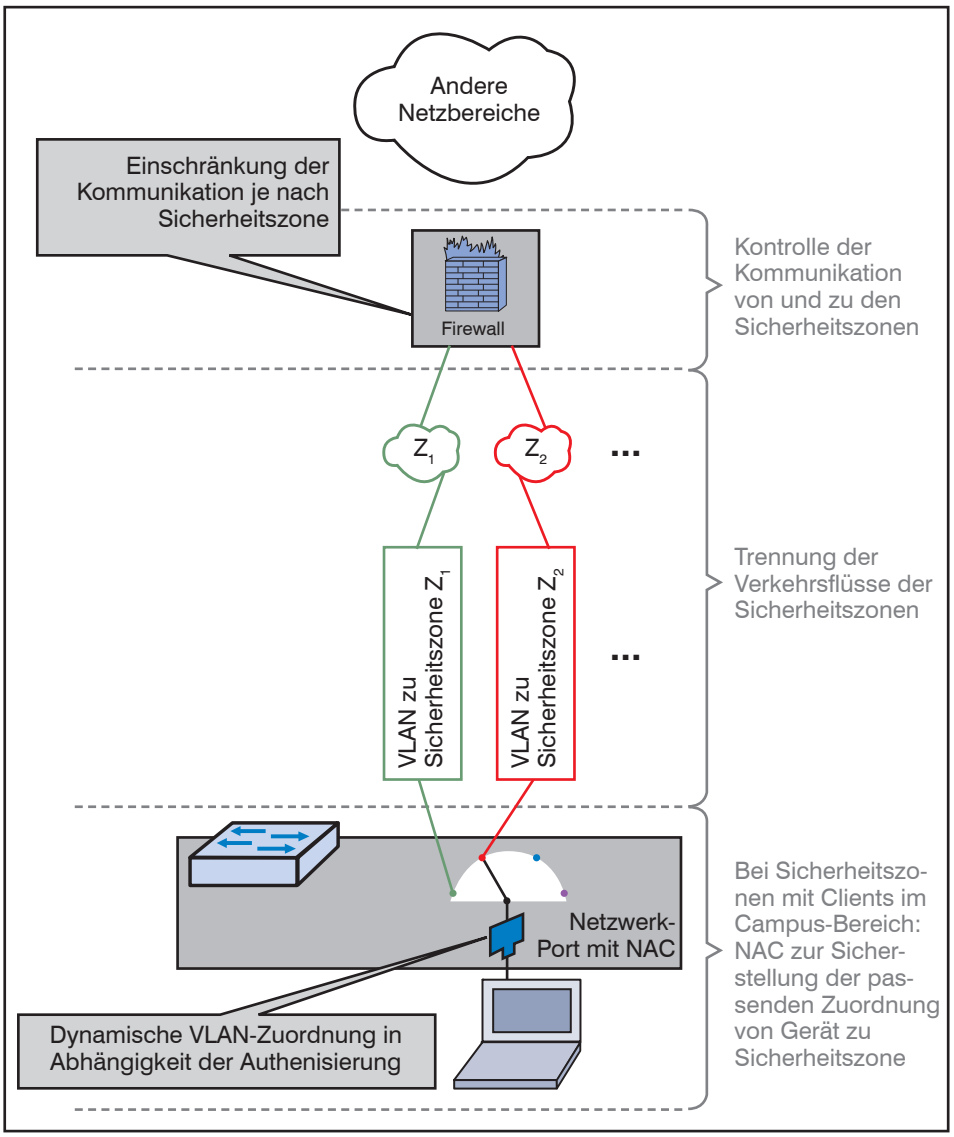


Abbildung 4: Elemente zum Aufbau einer Zonenarchitektur (Auswahl)

NAC ist immer dann notwendig, wenn durch andere Mechanismen (z.B. räumliche Trennung in Verbindung mit einer Zutrittskontrolle) eine passende Zuordnung von Endgerät und Mandantennetz nicht angemessen zugesichert werden kann.

Abbildung 4 stellt die beschriebenen Elemente zum Aufbau von Sicherheitszonen im Zusammenhang dar.

3. Kurzschlussvermeidung

Sobald ein Endgerät Schnittstellen in unterschiedliche Sicherheitszonen hat, besteht das Risiko eines Kurzschlusses der Zonenarchitektur, da ein Angreifer potentiell nun dieses Endgerät missbrauchen kann, um an einem Sicherheitselement vorbei von einer Zone zu einer anderen Zone zu gelangen. Die Vermeidung von bzw. der Umgang mit möglichen Kurzschlüssen ist ein wesentlicher Aspekt einer Zonenarchitektur, wie die im Folgenden diskutierten Beispiele zeigen.

Server-Anbindung

Im Normalfall wird ein Server für die produktive Kommunikation an eine einzelne Zone angebunden.

Es wird jedoch immer wieder vorkommen, dass Server Schnittstellen in unterschiedliche Sicherheitszonen haben (Dual-Homed Server). Was beim Aufbau von DMZs für die Anbindung z.B. von Gateways üblich ist, birgt bei internen Sicherheitszonen, wie eben beschrieben, die Gefahr eines Kurzschlusses der Zonenarchitektur (Abbildung 5).

Hier ist stets eine Einzelfallbetrachtung nötig. Man kann jedoch grob folgende Anforderungen für den Anschluss von Ser-

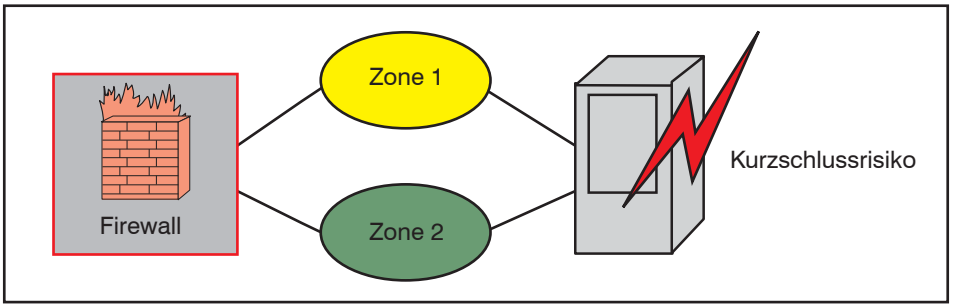


Abbildung 5: Kurschlussrisiko durch einen Server in unterschiedlichen Sicherheitszonen

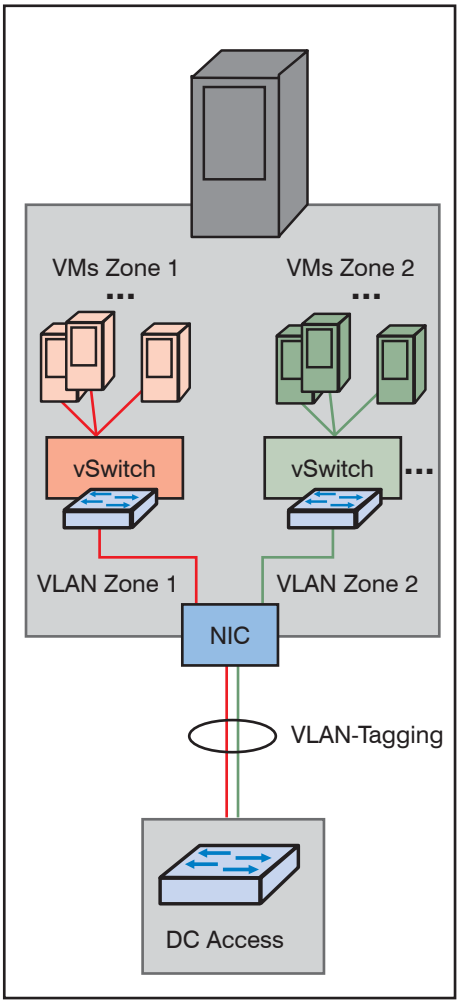


Abbildung 6: Beispiel einer Zonierung im Virtualisierungs-Host mit vSwitches

vern an unterschiedliche Sicherheitszonen stellen:

- Der Dual-Homed Server muss angemessen gehärtet sein. Der Härtungsgrad hängt vom Sicherheitsgefälle zwischen den Sicherheitszonen ab, an denen der Server angebunden ist.
- Es muss (zumindest bei Bedarf) jede Weiterleitung von Information zwischen den verbundenen Sicherheitszonen über den Dual-Homed Server nachvollziehbar kontrolliert werden können.
- Dual-Homed Server müssen auf Anwendungsebene die Kommunikation zwischen den Sicherheitszonen entkoppeln, insbesondere ist ein Routing zwischen den Sicherheitszonen über den Dual-Homed Server nicht gestattet.

Fortsetzung der Zonierung im Virtualisierungs-Host

In der Regel muss ein Virtualisierungs-Host (z.B. VMware ESX) Schnittstellen in unterschiedliche Sicherheitszonen erhalten. Die Segmentierung des Netzes in unterschiedliche Sicherheitszonen muss dann konsequent im Virtualisierungs-Host fortgesetzt und virtuelle Maschinen (VMs) auf dem Virtualisierungs-Host unterschiedlichen Zonen zugeordnet werden.

Hierzu wird auf dem Virtualisierungs-Host je Zone ein eigener virtualisierter Switch (vSwitch) konfiguriert und dem jeweiligen zonenspezifischen VLAN am Access Switch zugeordnet (Abbildung 6). Alternativ wird ein virtualisierter Switch verwendet, der unterschiedliche VLANs unterstützt und die virtuellen Ports für die VMs entsprechend ihrer Zonenzuordnung auf das jeweilige VLAN konfiguriert. Auf dem NIC des ESX-Host wird dann üblicherweise ein VLAN-Trunk konfiguriert.

Bei einem Cluster müssen die Sicherheitszonen entsprechend auf jedem Host des Cluster bereitgestellt werden und im Netz müssen die Zonen-VLANs entsprechend zur Verfügung stehen, wie in Abbildung 7 am Beispiel von VMware dargestellt.

Mainframe-Anbindung

Der Schutzbedarf des Mainframe ist bedingt durch die auf ihm verarbeiteten Daten meist zwingend als hoch einzustufen. Daher wird in der Praxis oft die Forderung gestellt, dass der Mainframe auf Grund seiner Kritikalität einer Sicherheitszone zugeordnet wird, die zumindest den Mainframe von Clients und eingeschränkt vertrauenswürdigen Servern abschottet.

Wenn unterschiedliche virtuelle Umgebungen auf dem Mainframe bestehen, müssen diese ggf. auch hinsichtlich der Zonenzugehörigkeit unterschieden werden. Der Mainframe kann also ggf. mehreren Sicherheitszonen zugeordnet werden. Dabei ist sicherzustellen, dass der Mainframe nicht als Router (z.B. OSPF Member) konfiguriert ist, was in der Pra-

Seminar

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001
09.09. - 11.09.13 in Bonn

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance“-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam“ zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice“-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter“ Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Referenten: Dr. Simon Hoff, Dipl.-Inform. Oliver Flüs
Preise: € 1.890,-- netto

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

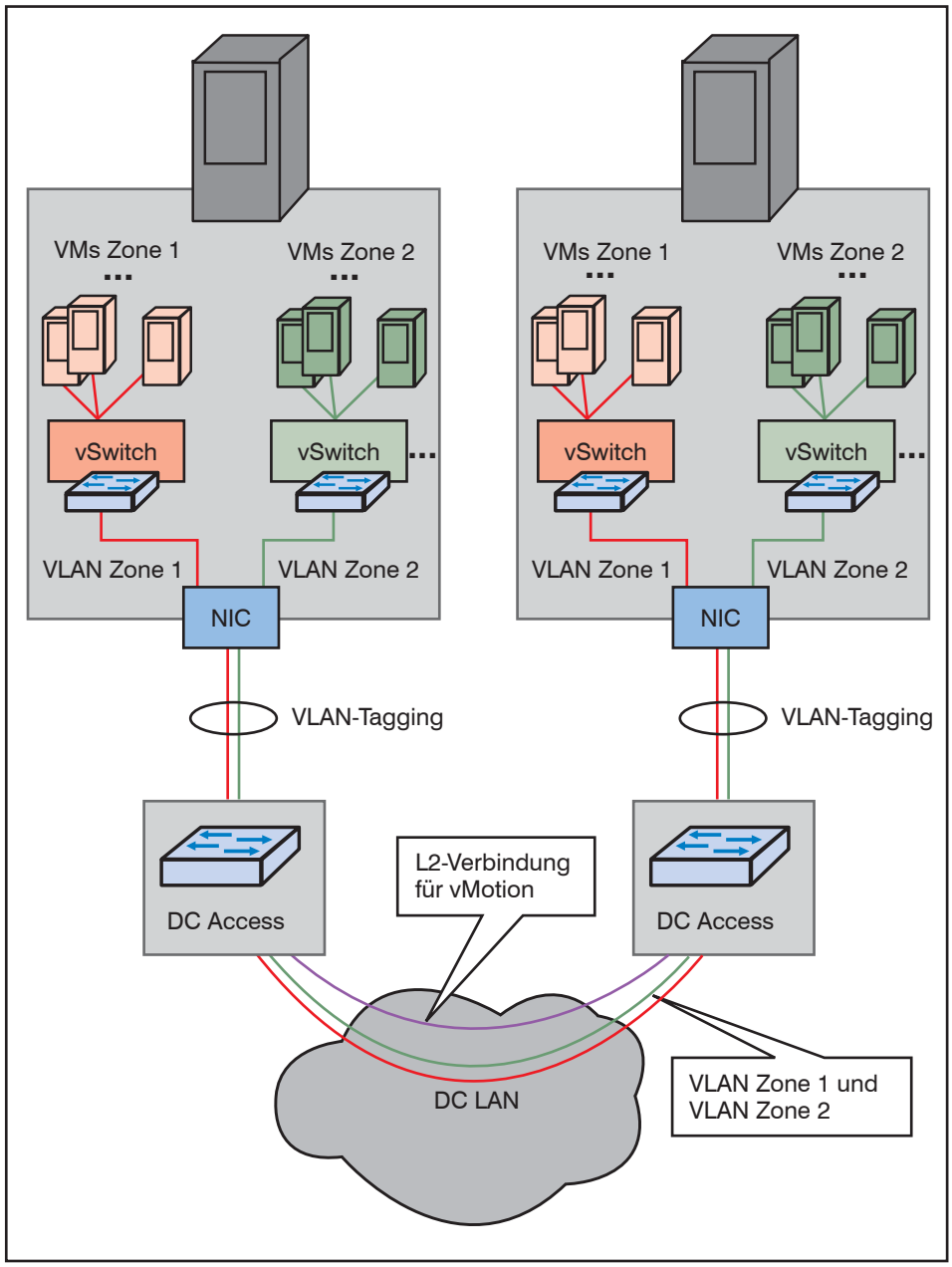


Abbildung 7: Zonen bei einem ESX Cluster

xis durchaus vorkommt, denn sonst würde der Mainframe die Sicherheitszonen per Routing kurzschließen können.

Load-Balancer-Anbindung

Es gibt – unabhängig von Zonenarchitekturen – unterschiedliche Anbindungsformen für einen Load Balancer (LB). Beispiele sind:

- Network Address Translation (NAT): Beim Verwendung von NAT tauscht der LB lediglich die Ziel-IP-Adresse einer Client-Anfrage. Die Quell-IP des Clients bleibt unverändert. Dies funktioniert nur, wenn sichergestellt ist, dass die Antwort des Servers (die direkt an den Client gerichtet ist) den LB passiert, damit dieser die Quell-IP-Adresse des Antwortpakets auf seine eigene Adresse abändern kann. Dazu wird der LB als Default-Gateway vor die realen Server geschaltet. Dann kann der LB die IP-Adresse wieder tauschen und das Paket entsprechend routen.

- Source-NAT (SNAT), auch Proxy-IP (PIP) genannt: LBs werden hier one-armed über ein einzelnes Interface angeschlossen, d.h. sie werden wie Server behandelt. Dabei tauscht der LB sowohl die Quell- als auch die Ziel-IP Adresse der Client-Pakete. Die Quell-IP des Clients wird durch die IP-Adresse des LB und die Ziel-IP-Adresse wird durch die Adresse des ausgewählten Servers ersetzt.

LBs in einer Zonenarchitektur könnten nun pro Sicherheitszone vorgesehen werden, was bei steigender Anzahl von Sicherheitszonen jedoch schnell die Grenzen der Wirtschaftlichkeit sprengt.

Daher ist es meist attraktiv zu überlegen, ob ein LB mehrere Sicherheitszonen versorgen darf. (siehe Abbildung 8) Damit gibt es zunächst wieder das bekannte Kurzschlussrisiko. Der LB muss also entsprechend gehärtet und durch sorgfältige Konfiguration muss das Risiko minimiert werden. Je nach Hersteller wird auch die Möglichkeit von virtuellen LBs (oder einer ähnlichen Funktion) angeboten. In diesem Fall kann ein virtueller LB pro Sicherheitszone vorgesehen werden. (siehe Abbildung 9).

Storage-Anbindung

Auch bei einer Anbindung an ein Storage Area Network (SAN) besteht grundsätzlich ein Kurzschlussrisiko, das allerdings durch eine geeignete Zonierung mit SAN-Bordmitteln erreicht werden kann. Bei SANs auf Basis von Fiber Channel (FC) besteht zusätzlich noch eine technologiebedingte starke Trennung zwischen IP-Netzen und SANs. Bei FC over Ethernet (FCoE) hängt das Risiko von der Netzkonfiguration ab. Werden Switches exklusiv für FCoE genutzt, ist man aus einer Sicherheitsperspektive wieder recht nah an FC herangerückt. Andernfalls müssen auf den Switches zusätzliche Sicherheitsmaßnahmen umgesetzt werden, um das Risiko zu minimieren.

Interessanter ist da schon die NAS-Anbindung. Wie bei der Betrachtung zum Thema Load Balancer ist der Einsatz eines NAS Filer pro Sicherheitszone in den meisten Fällen aus wirtschaftlichen Gründen nicht möglich. Wenn ein NAS Filer nun an mehrere Sicherheitszonen angeschlossen werden soll, muss der Filer sicherheitstechnisch zunächst wie ein Server behandelt werden und stellt natürlich ein Kurzschlussrisiko dar. Ein Filer muss daher entsprechend gehärtet werden. Sofern vom Hersteller unterstützt, sollte möglichst mit einem virtuellen Filer (vFiler) pro Sicherheitszone gearbeitet werden, wie in Abbildung 10 dargestellt.

4. Festlegung der Sicherheitszonen

Bei der Festlegung der initialen Sicherheitszonen einer Zonenarchitektur ist Vorsicht geboten. Im Sinne von „weniger ist mehr“ sollten nur die wirklich benötigten Sicherheitszonen angelegt und schrittweise mit Leben gefüllt werden. Es

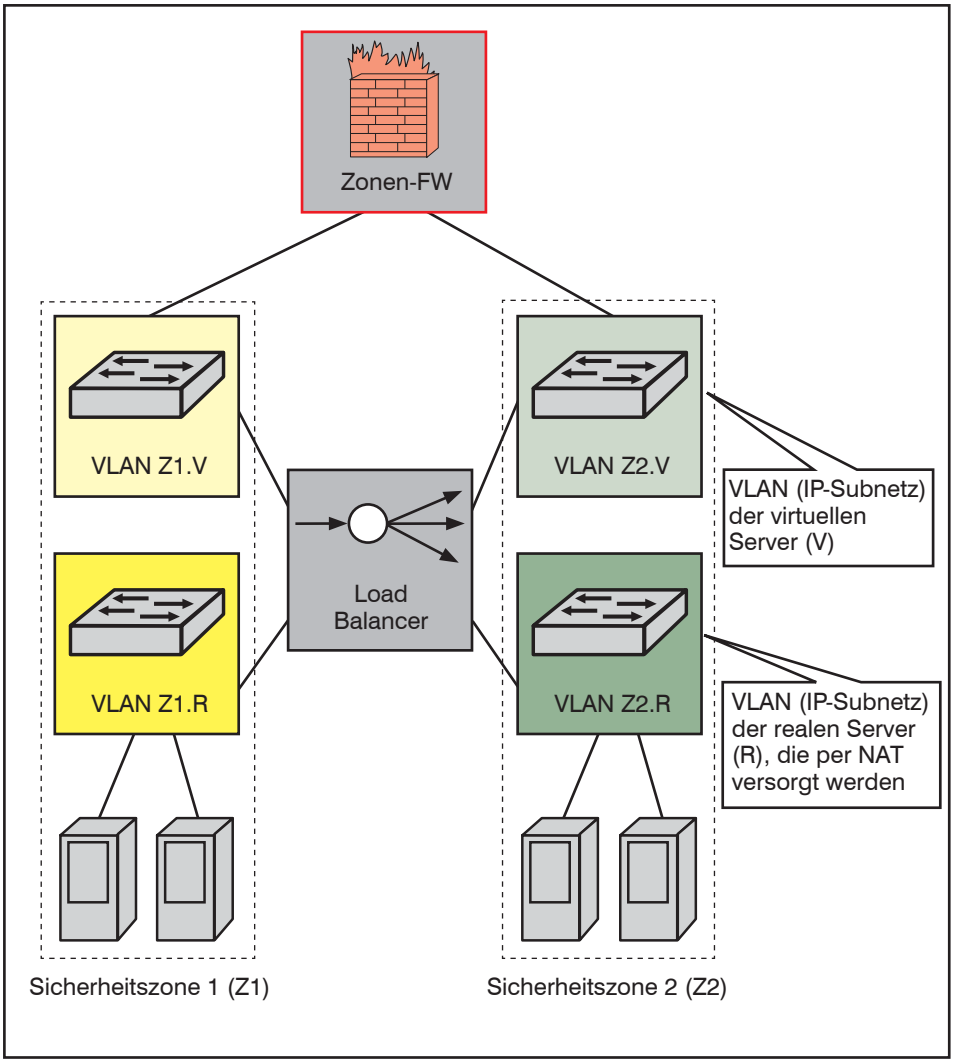


Abbildung 8: Anschaltung Load Balancer an mehrere Sicherheitszonen unter Verwendung von NAT

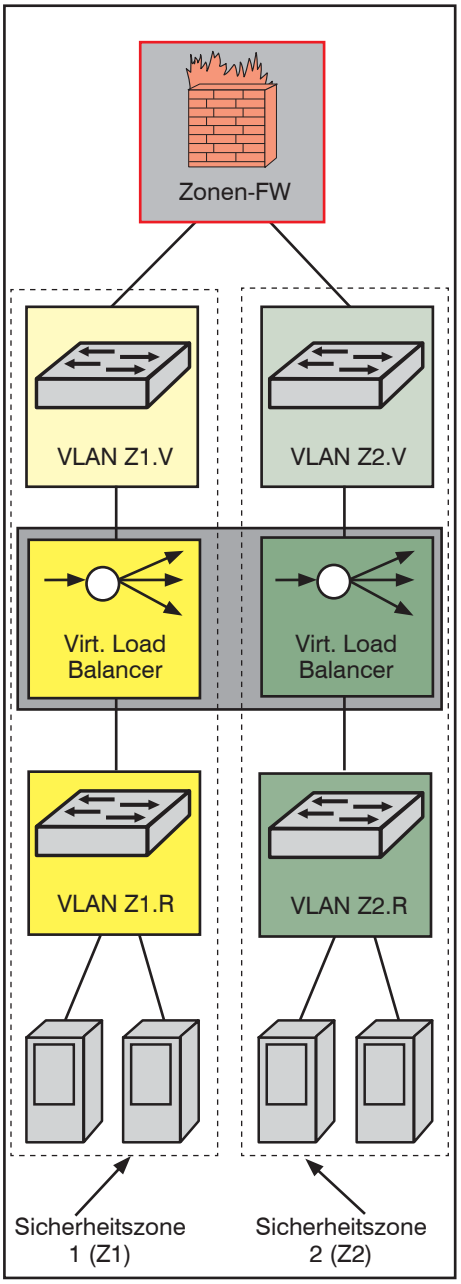


Abbildung 9: Verwendung virtueller Load Balancer

ist allerdings damit zu rechnen, dass bedarfsorientiert weitere Sicherheitszonen hinzuzufügen sind. Daher ist zu empfehlen, zur besseren Strukturierung unterschiedliche Typen von Sicherheitszonen zu spezifizieren. Beispiele sind:

- Aufteilung nach Clients und Servern: Sicherheitszonen mit virtuellen Clients und ggf. (virtuellen) Servern und Sicherheitszonen, in denen sich ausschließlich (virtuelle) Server befinden

- Aufteilung nach Vertrauensgrad: hohes Vertrauen (Trusted), geringes Vertrauen (Untrusted) und ggf. Restricted für eingeschränktes Vertrauen

Mit diesen Festlegungen lassen sich bei Bedarf dann auch Entwicklungs- und Testsysteme von produktiv genutzten Systemen trennen, wobei z.B. eine Sicherheitszone für Entwicklung und Test und eine weitere Sicherheitszone für Vorproduktion/Staging und IT-Produktion vorgesehen wird. Eine solche Anforderung wird ebenfalls von ISO 27001 gestellt (siehe Maßnahme A.10.1.4 in ISO 27001), die Trennung kann jedoch durch entsprechende Berechtigungskonzepte auch auf Ebene von Betriebssystem oder Plattform der beteiligten Systeme erfolgen.

Es ist empfehlenswert als Basis zunächst folgende Sicherheitszonen in Betracht zu ziehen:

- **Standard-Client-Server-Zone:** Hier werden alle Systeme (Clients und Server) zusammengefasst, für die (noch) keine spezifischen Zonierungsanforderungen bestehen. Im Initialzustand kann diese Zone mit dem Office-Netz oder sogar dem Intranet einer Institution übereinstimmen. Schrittweise können dann Systeme aus dieser Sicherheitszone in andere Sicherheitszonen migriert werden.

- **Standard-Server-Zone:** Hier werden alle Server positioniert, die zwar separiert werden sollen, für deren Zonierung aber keine speziellen, weitergehenden Anforderungen bestehen.

- **Common-Services-Zone:** Server, die allgemein verfügbare Dienste anbieten (z.B. DNS, LDAP, Active Directory) werden hier positioniert.

- **VDI-Zone:** Für virtualisierte Clients, die als VM von einer Virtual Desktop Infrastructure bereitgestellt werden, wird oft eine separate Sicherheitszone vorgesehen, da eine VDI-Lösung ja zentral im RZ aufgebaut wird und damit Client-Logik ebenfalls zentral im RZ läuft. Ansons-

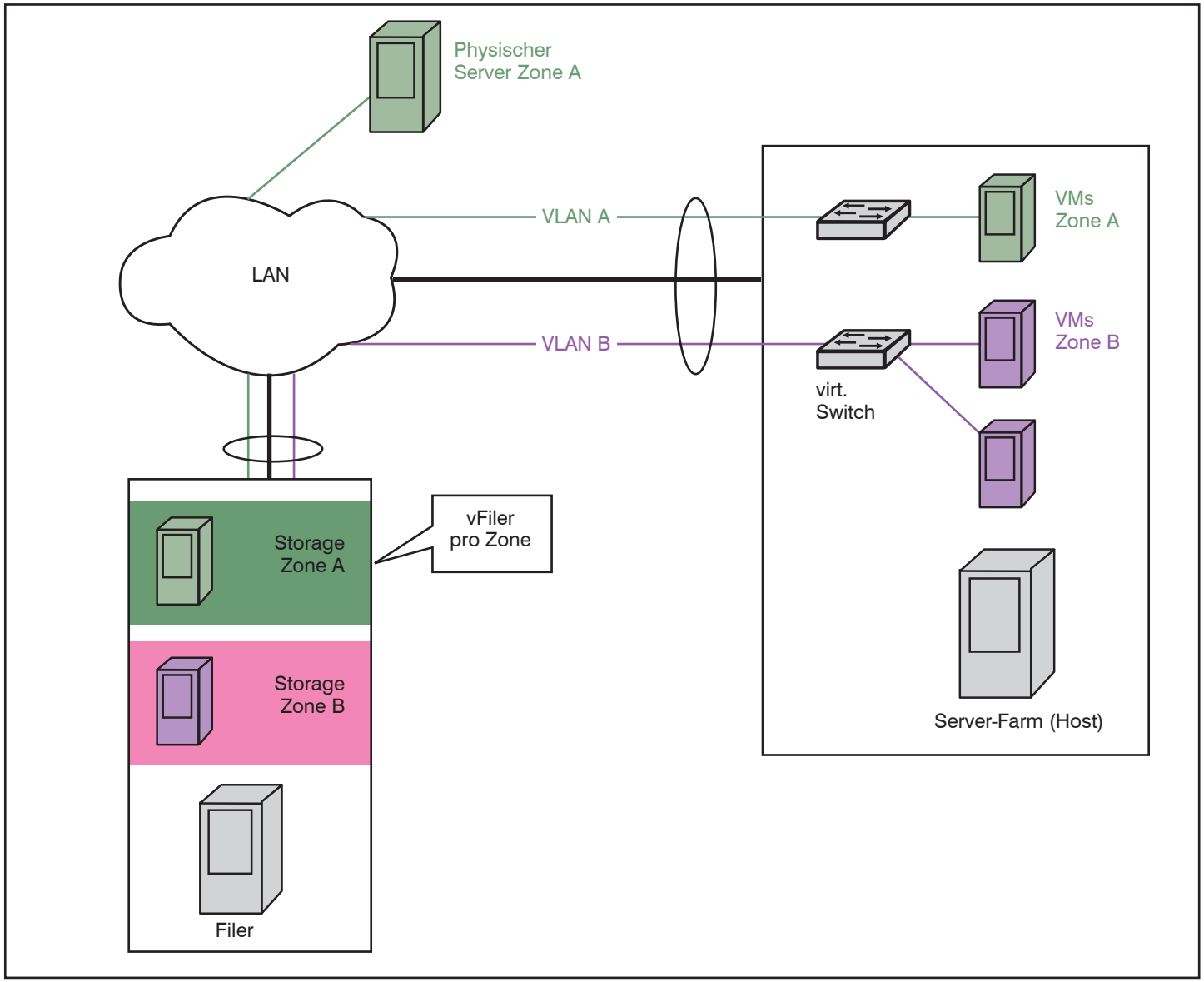


Abbildung 10: Verwendung von virtuellen Filern pro Sicherheitszone

ten könnte eine schadenstiftende Software, die eine Client-VM befällt, sich im RZ ungehindert weiter ausbreiten. Alternativ können Client-VMs auch der Standard-Client-Server-Zone zugeordnet werden.

- **Anwendungs-Virtualisierungs-Zone:** Terminal Server, die Anwendungen bereitstellen, werden mit einem zur VDI-Zone analogen Argument oft ebenfalls per Default separiert. Alternativ können die Server auch der VDI-Zone oder der Standard-Client-Server-Zone zugeordnet werden.

Abbildung 11 zeigt exemplarisch die beschriebene Zonenaufteilung.

5. Konflikte zwischen Netz- und Host-basierten Sicherheitszonen

Das Domänenkonzept von Microsoft stellt ein klassisches Host-basiertes Zonenkonzept dar, bei dem Authentisierung und gruppenbasierte Berechtigungen für Windows-Systeme durch Active Directory (AD) / Domain Controller (DC) erfolgen. Eine Domäne stellt dabei ein Vertrauensbereich dar, vergleichbar zu einer Sicherheitszone. Das Domänenkonzept basiert daher auf der Arbeitsannahme, dass innerhalb einer Domäne der Verkehr nicht weiter gefiltert werden muss. Da die Kommunikation mit AD/DC in höchstem Maße komplex ist, ist außerdem eine Filterung der Kommunikation z.B. an einer Firewall entsprechend schwierig.

Hier kollidiert das Domänenkonzept von Microsoft automatisch mit einem netzbasierten Zonenkonzept. An dieser Stelle wird nicht selten gefordert, dass am besten jegliche Zonierung Host-basiert zu erfolgen habe. Das Netz möge sich auf Transportaufgaben konzentrieren, nicht mehr und nicht weniger. Das hört sich zwar gut an, ist aber unrealistisch, da es nicht konsequent umsetzbar ist.

Es bleibt also bis auf weiteres eine Tatsache, dass wir mit dem Konflikt der diametralen Zonenkonzepte leben müssen. Eine Firewall hat dann kaum eine andere Wahl als die Kommunikation zwischen Windows-Systemen und AD/DC sowie zwischen AD/DCs entsprechend freizuschalten.

Noch extremer ist der Widerspruch bei Verwendung einer Ende-zu-Ende-Verschlüsselung zwischen Hosts. Ein Beispiel ist Microsoft Domain and Server Isolation. Hier wird Host-basiert mit IPsec die Kommunikation abgesichert und optional sogar verschlüsselt (d.h. die IPsec Security As-

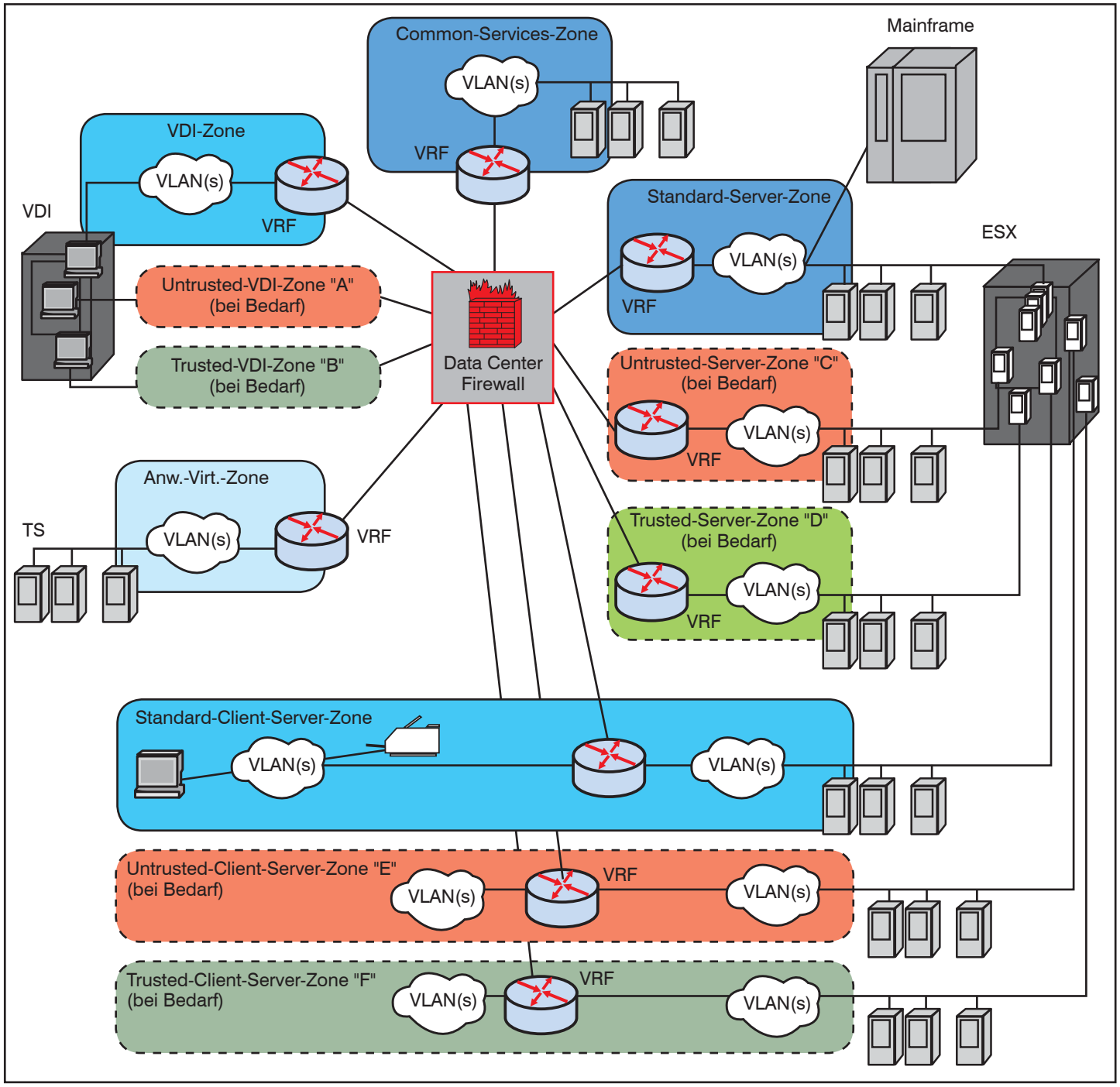


Abbildung 11: Beispiel für eine Intranet-Zonenarchitektur

sociations bestehen direkt zwischen den Hosts). Ein Firewall-System hat nun keine Möglichkeit mehr den Verkehr zu inspizieren.

6. Management der Sicherheitszonen

Die Administration von IT-Systemen ist naturgemäß eine machtvolle Aufgabe, die missbräuchlich durchgeführt einen erheblichen Schaden verursachen kann.

Daher ist eine typische Forderung die Trennung von Systemen, die zur Administration und Überwachung der Infrastruktur dienen, von funktional genutzten Systemen. Hierzu sind dann entsprechende Managementzonen vorzusehen.

Absicherung des Zugangs zu Managementzonen

Der Zugang zu Managementzonen muss mit starken Sicherheitsmaßnahmen abgesichert werden. Typisch sind hier eine starke Authentisierung und die Protokollierung von Sitzungsdaten und ggf. sogar vollständiger Administrationssitzungen. Außerdem ist oft eine starke Entkopplung von administrativen Zugriffen (speziell bei Zugriffen durch externe Unternehmen) gewünscht. Bei der Entkopplung administrativer Zugriffe werden inzwischen gerne Terminal Server und VDI eingesetzt.

Aus Verfügbarkeitsgründen ist es durchaus gängig den Zugang zu Managementzonen über eine eigene Firewall zu regeln (Management Firewall). Es gibt aber genauso Installationen, die für die Kontrol-

le des Managementzugriffs die produktive Data Center Firewall nutzen.

Funktionale Strukturierung der Managementzonen

Je nach Managementaufgabe werden die Sicherheitszonen oft funktional in Sicherheitszonen für Firewall-Management, Management von Virtualisierungslösungen, Server-Management, Netzmanagement, etc. aufgeteilt.

Außerdem werden üblicherweise unterschiedliche Zugriffsformen (z.B. Management-Ethernet-Port oder serielle Schnittstelle / Konsolen-Port, integrated Lights Out (iLO) – oder vergleichbare Technologie) auf die zu verwaltenden Geräte separiert.

An der Management Firewall können daher beispielsweise folgende Zonen etabliert werden (siehe Abbildung 12):

- Zugangszonen für Authentisierung und Entkopplung der Kommunikation
- Managementzonen für Managementserver (z.B. für Netzmanagement, Überwachung)
- FW-Managementzone
- Zonen für die Anbindung der zu administrierenden Geräte, z.B.:
  - pro funktionaler Sicherheitszone eine Zone iLO (oder vergleichbar) für Unix / Linux, Windows und ESX (oder vergleichbar) im Intranet und im Data Center
  - pro Cluster eine Zone vCenter für VMware (oder vergleichbar)
  - eine ggf. gemeinsame Zone für KVM-Switches (KVM ist die Abkürzung für Keyboard, Video and Mouse)
  - eine separate Zone für Mainframe-Administration
  - pro funktionaler Zone eine Zone für den Zugriff auf Management-Ports von Switches

Weiterhin erfolgen meist Anbindungen an alle funktionalen Zonen für ein Inband-Management.

7. Migrationsaspekte

Außerhalb der grünen Wiese ist die Migration zu einer Zonenarchitektur ein langfristiges, strategisches Unterfangen. Einer der Gründe ist, dass im Regelfall die Änderung von IP-Adressen produktiver Server (was ein Umzug in eine Sicherheits-

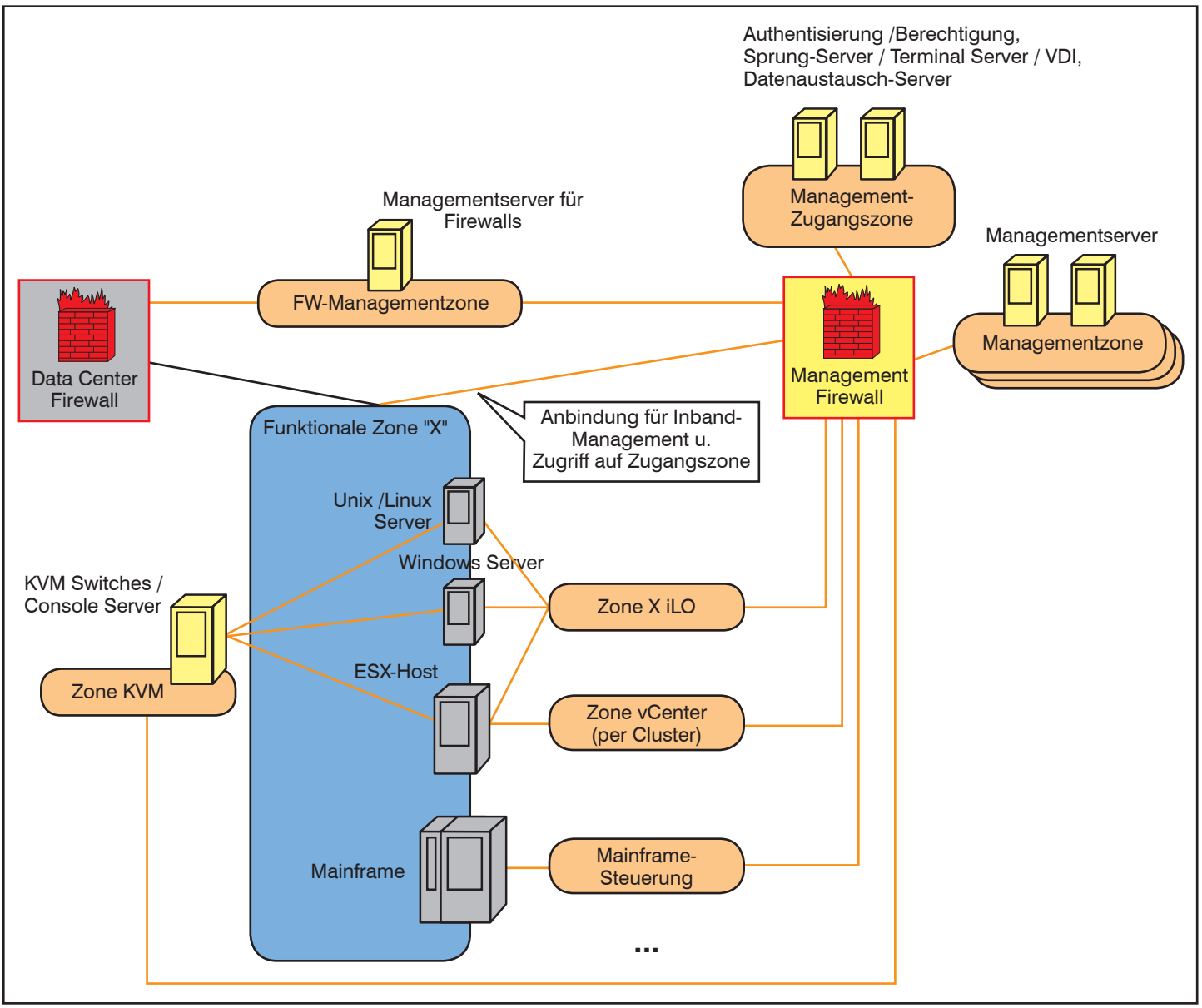


Abbildung 12: Beispiel für den Aufbau von Managementzonen

zone ggf. erfordern könnte) aus Gründen der Betriebssicherheit ausgeschlossen ist.

Die Migration einer bestehenden Infrastruktur basiert daher meist auf den folgenden Elementen:

- Clients, die per DHCP mit IP-Adressen versorgt werden, können vergleichsweise einfach in ein anderes IP-Netz umgezogen werden. Bei der Verwendung von statischem DHCP ist der Aufwand allerdings etwas größer. Daher ist eine übliche Strategie für die Trennung von Clients und Servern in unterschiedliche Sicherheitszonen zunächst die Clients in neue IP-Netze umzuziehen, die dann an der Data Center Firewall gefiltert werden können.

- Wenn Server bereits in eigenen IP-Subnetzen gehalten werden, kann versucht werden diese Subnetz en bloc derart zu migrieren, dass die Server zwar ihre IP-Adresse behalten, jedoch eine Firewall vor ihrem Subnetz platziert ist (die dann je nach Konfiguration als Default Gateway für die Server auftritt).

- Bei der Beschaffung neuer IT-Systeme wird bereits bei der Planung die Zonierung berücksichtigt, damit die Systeme von Anfang an der gewünschten Sicherheitszone zugeordnet werden.

8. Betriebsprozesse

Für die nachhaltige Umsetzung einer Zonenarchitektur ist die Berücksichtigung und entsprechende Anpassung der Betriebsprozesse von entscheidender Bedeutung.

Insbesondere ist zunächst die Etablierung eines Prozesses (bzw. eine entsprechende Erweiterung eines bestehenden Prozesses) zur **Schaffung neuer Sicherheitszonen** erforderlich. Dies beinhaltet unter anderem die folgenden Punkte:

- Festlegungen zur Zuständigkeit für die Schaffung einer neuen Sicherheitszone: Typischerweise ist hier die Erstellung einer Entscheidungsvorlage in der Verantwortung des Sicherheitsbeauftragten und die Entscheidung liegt bei dem entsprechenden Management Board für die Informationssicherheit.

- Dokumentation: Mit der Beantragung einer neuen Sicherheitszone muss eine Beschreibung der Schutzziele, die mit der neuen Zone verbunden sind, erfolgen und die Kriterien zur Server- bzw. Client-Zuordnung müssen spezifiziert werden.

Eine ähnliche Situation ergibt sich bei der Einführung von neuen Anwendungen. Auch hier muss der bereits bestehende Prozess um Punkte ergänzt werden, die spezifisch für Zonenarchitekturen sind:

- Es muss identifiziert werden, welche bestehenden und neuen IT-Systeme (Clients, Server) von der Anwendung betroffen sind.

- Neue IT-Systeme müssen den Sicherheitszonen zugeordnet werden.

- Regelwerke auf Firewalls müssen ergänzt und ggf. IPS-Policies angepasst werden.

Für Sicherheitszonen müssen natürlich auch Changes bearbeitet werden. Besonders wichtig ist dabei, dass bei **Changes von IT-Systemen und Anwendungen** geprüft wird, ob der Change von der Zonenarchitektur betroffen ist. Ein entsprechender Prüfpunkt muss zwingend im Change-Prozess berücksichtigt werden. Wenn z.B. ein Software Update eines IT-Systems oder einer Anwendung auch eine Anpassung einer Firewall-Regel oder einer IPS Policy erfordern würde, eine entsprechende Prüfung aber nicht Bestandteil des Prozesses ist, kann die Änderung auf dem Sicherheitselement übersehen werden und der Update scheitern bzw. Anwendungsfehler die Folge sein.
Auch die Prozesse im User Help Desk und im 2nd Level Support müssen um die Aspekte der Zonenarchitektur ergänzt werden. Dabei wird die ohnehin schon hohe Komplexität des Troubleshooting um eine weitere Dimension ergänzt. In der Praxis zeigt sich leider immer wieder, dass es sehr schwer sein kann, Fehler zu lokalisieren und zu analysieren, die ihre Ursache letztendlich im Verhalten einer Firewall oder eines anderen Sicherheitselements haben.

9. Fazit

Je unüberschaubarer die Landschaft der IT-Systeme in RZ und Campus wird, desto intensiver wird die Informationssicherheit eine Zonenarchitektur fordern. Dabei geht es primär um eine notwendige Ordnungspolitik und der damit verbundenen Reduktion der Angriffsfläche.

Die Komplexität einer solchen Zonenarchitektur ist allerdings erheblich und immer wieder sind Sonderbetrachtungen für den Umgang mit einem potentiellen Kurzschluss der Sicherheitszonen durch IT-Systeme, die an mehrere Zonen angebunden werden, notwendig. Als Folge gestalten sich Migration und Betrieb ebenfalls als aufwendig.

Alternativen zu einer netzbasierten Zonenarchitektur gibt es derzeit jedoch im Regelfall nicht. Damit ist letztendlich das Herz einer Zonenarchitektur stets eine entsprechend dimensionierte, leistungsfähige Data Center Firewall. Die Herausforderungen an Verfügbarkeit, Leistung und Qualität sind hier immens und es ist

Seminar

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001
09.09. - 11.09.13 in Bonn

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance“-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam“ zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice“-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter“ Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Referenten: Dr. Simon Hoff, Dipl.-Inform. Oliver Flüs
Preise: € 1.890,-- netto

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

hier durchaus die Frage zu stellen, ob die Firewall-Hersteller dem auch gewachsen sind.

10. Abkürzungen

ACL	Access Control List
BSI	Bundesamt für Sicherheit in der Informationstechnik
DC	Data Center
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FC	Fiber Channel
FCoE	FC over Ethernet
IEEE	Institute of Electrical and Electronics Engineers
iLO	integrated Lights Out
IP	Internet Protocol
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization
KVM	Keyboard, Video and Mouse
LAN	Local Area Network
LB	Load Balancer
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MACsec	MAC Security
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NGFW	Next Generation Firewall
NIC	Network Interface Card
OSPF	Open Shortest Path First
IP	Proxy-IP
RADIUS	Remote Authentication Dial-In User Service
RTP	Real-Time Transport Protocol
RZ	Rechenzentrum
SAN	Storage Area Network
SGACL	Security Group ACL
SGT	Security Group Tag
SNAT	Source NAT
TOGAF	The Open Group Architecture Framework
UDP	User Datagram Protocol
UHD	User Help Desk
VDI	Virtual Desktop Infrastructure
VLAN	Virtual LAN
VM	Virtual Machine
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN

11. Literatur

[1] DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren Informationssicherheit-Managementsystem – Anforderungen, 2008

[2] IEEE 802.1AE-2006, „Media Access Control (MAC) Security“, August 2006, verfügbar unter http://www.ieee.org

[3] IEEE 802.1X-2010, „Port-based Network Access Control“, Februar 2010, verfügbar unter http://www.ieee.org

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), „IT-Grundschutz-Kataloge“, 12. Ergänzungslieferung, 2011, verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Download/download_node.html

[5] VMware, “vSphere 5.1 Security Hardening Guide”, verfügbar unter http://www.vmware.com/support/support-resources/hardening-guides.html

[6] Gartner, „Defining the Next-Generation Firewall“, Gartner Research Note, 12.10.2009

Kongress

ComConsult IT-Sicherheits-Forum 2013
23.09. - 24.09.13 in Euskirchen

Das ComConsult IT-Sicherheits-Forum 2013 konzentriert sich auf folgende Themenbereiche: Konsequenzen von SDN auf Sicherheitsinfrastrukturen, Sicherheit im Internet of Things, das vernetzte Fahrzeug, Cloud Sichere Nutzung und Aufbau von Clouds, Sicherheit in UCC, Gefährdungen bei IPv6, Sichere Identitäten in IP-Netzen, Network Access Control (NAC) in der Praxis Mandantenfähigkeit und Zonenkonzepte in RZ und Campus, Sicherer Betrieb von IT-Infrastrukturen: Authentisierung, Berechtigung, Protokollierung und Entkopplung der Kommunikation.

Das IT-Sicherheits-Forum 2013 konzentriert auf folgende Themenbereiche:

- Konsequenzen von Software Defined Networking (SDN) auf Sicherheitsinfrastrukturen
- Sicherheit im Internet of Things – Konsequenzen der Verwendung von Standard-IT-Komponenten
- Das vernetzte Fahrzeug: Welche Möglichkeiten bereits heute bestehen, welche Gefährdungen hieraus resultieren und wie mit ihnen umgegangen werden kann
- Cloud Computing: Sicherer Nutzung von Clouds, Aufbau sicherer private Clouds und Anforderungen an sichere Public Clouds
- Konzentration auf Information: Verschlüsselung von Daten bei Transport und Speicherung, Datenklassifikation, Data Loss Prevention und Revisionsfähigkeit
- Sicherheit in UCC: Umgang mit dem Zielkonflikt zwischen möglichst flexibler Zusammenarbeit und der Absicherung der Daten
- Gefährdungen bei IPv6 und welche Maßnahmen heute möglich sind
- Sichere Identitäten in IP-Netzen
- Network Access Control (NAC) in der Praxis
- Mandantenfähigkeit und Zonenkonzepte in RZ und Campus: Netz- und Firewall-Architekturen, Server- und SAN/NAS-Anbindung
- Sicherer Betrieb von IT-Infrastrukturen: Authentisierung, Berechtigung, Protokollierung und Entkopplung der Kommunikation

Wie auch in den Vorjahren greift das IT-Sicherheits-Forum 2013 die aktuellsten Entwicklungen im Bereich der Informationssicherheit auf.

Moderation: Dr. Simon Hoff
Preise: € 1.690,-- (statt € 1.890,--)*
*rabattierter Preis gültig bis zum 31.07.2013

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Standpunkt Troubleshooting

Jumbo Frames als „Nachbrenner“?

Der Standpunkt Troubleshooting von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Sie erinnern sich: Mit Gigabit Ethernet erblickte eine neue Technik das Licht der Welt, die landläufig unter der Bezeichnung „Jumbo Frames“ bekannt wurde. Die Idee dahinter war, dass eine Station, die große Datenmengen zu übertragen hat, weniger Pakete aussenden muss, wenn diese größer als die bei Ethernet sonst übliche Grenze von 1514 Byte sind. Und in der Tat findet man aus dieser Zeit (also vor etwa 10 Jahren) verschiedene Veröffentlichungen, die den Einsatz von Jumbo Frames für Hochleistungssysteme nahelegen. Die Beobachtung war nämlich, dass die damals aktuelle Server Hardware nicht in der Lage war, einen Gigabit-Ethernet-Adapter voll auszulasten, solange die normale Ethernet-Paketgröße verwendet wurde.

Dabei geht es weniger um die Einsparung von Bytes als vielmehr um die Verarbeitung der Pakete. Der Overhead, d.h. das Verhältnis von Paketheadern zur Nutzlast, verringert sich nämlich durch die Jumbo Frames um höchstens 4%. Dabei muss jedoch nur noch ein Sechstel der Paket-Header (Ethernet MAC, IP, TCP, etc.) von den Endgeräten verarbeitet werden.

Soweit so gut. Irgendwie ist es still um das Thema geworden. Die schnelle Entwicklung der Server Hardware hat diesen Nachteil offensichtlich schnell hinter sich gelassen. Gigabit Ethernet stellt mittlerweile nicht einmal mehr für mittelmäßige Notebooks ein Problem dar. Aber Totgesagte leben länger. Plötzlich poppt das Thema wieder auf. Jetzt möchten nämlich die RZ-Betreiber ihre 10-Gigabit-Adapter voll auslasten. Und dafür wären doch Jumbo Frames ein probates Mittel, oder?

So wurde ich also neulich gefragt, ob ich das empfehlen könne. Um genau zu sein, hatte man Jumbo Frames auf kritischen Komponenten aktiviert, um die Datensicherung zu beschleunigen. Leider funktionierten danach bestimmte Anwendungen nicht mehr.

Ich habe also zunächst den Ethernet-Standard (IEEE 802.3 in der Ausgabe von 2008) hervorgeholt. Und – tatsächlich – auf knapp 3000 Seiten taucht der Begriff „Jumbo“ überhaupt nicht auf! Besser noch: Der Standard schreibt klipp und klar, dass die von einem Ethernet-Adapter zu unterstützende maximale Paketgröße 1514 Byte beträgt. Oder 1518 Byte, wenn VLAN Tags zu übertragen sind. Oder 2000 Byte, wenn Ethernet im Zusammenhang mit Layer-2-Enkapsulierungstechniken verwendet wird, z.B. beim Provider Backbone Bridging (PBB). Von Paketen, die 4088 oder gar 9216 Byte lang sind, ist nicht die Rede. Es gibt eine Ausnahme: Wenn Gigabit Ethernet im Halb-Duplex-Modus betrieben wird, können mehrere Pakete hintereinander gehängt werden, ohne dass ein neuer Medienzugang erforderlich wäre. Es entsteht ein „Burst“, der maximal 8192 Byte umfassen darf. Halb-Duplex bei Gigabit Ethernet braucht aber – sind wir ehrlich – kein Mensch.

Dennoch, was spricht dagegen, Jumbo Frames einzusetzen, obwohl sie im Ethernet-Standard nicht erwähnt werden? Im Prinzip nichts! Aber bedenken Sie: Zwischen Endgeräten in einem Ethernet-Segment gibt es kein Verfahren, sich auf eine maximale Paketgröße zu einigen. Solche Verfahren funktionieren nur im Zusammenhang mit Routern, die schon immer darauf ausgelegt waren, Netze unterschiedlicher Technik und Paketgröße miteinander zu verbinden. Typische Verfahren im Zusammenhang mit Routern sind IP-Fragmentierung und Path MTU Discovery (RFC 1191). Diese Verfahren basieren aber darauf, dass die Schnittstelle eines Routers die Pakete entgegennimmt und verarbeitet. Unterstützt diese Schnittstelle keine Jumbo Frames, wird sie solche einfach verwerfen. Fazit: Alle zu einer Broadcast-Domäne gehörenden Endgeräte müssen dieselbe maximale Paketgröße unterstützen, Switches eingeschlossen.

Diese Forderung wird sich aber im Allgemeinen schwer durchsetzen lassen. Insbesondere Broadcast-Domänen in Rechenzentren werden ja seit einigen Jahren immer größer. Es dürfte also einer Sysiphosarbeit gleichkommen, alle Adapter auf dieselbe Jumbo-Paketgröße einzustellen und danach sicherzustellen, dass diese Einstellung an keinem neuen Gerät vergessen wird. Kurz gesagt, ich halte das nicht für realistisch. So bleiben Sie also besser bei der Standardeinstellung und vertrauen darauf, dass schon in wenigen Jahren ihre Server-Hardware so leistungsfähig ist, dass es wieder still um die Jumbo Frames wird.

Seminar

Trouble Shooting in vernetzten Infrastrukturen 24.09. - 27.09.13 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Referenten: Dipl.-Inform. Oliver Flüs, Dr.-Ing. Joachim Wetzlar
Preise: € 2.290,-- netto

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Seminar*plus*

IPv6 Grundlagen
mit neuem Seminarkonzept

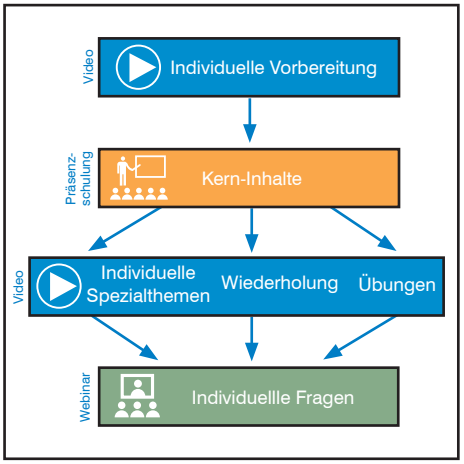
Die ComConsult Akademie veranstaltet vom 16.09. - 17.09.13 ihr Seminar*plus* "IPv6 Grundlagen" in Berlin.

IPv6 ohne die notwendigen Grundlagen zu planen oder gar zu betreiben, entspricht einem Blindflug ohne Flugerfahrung: zu groß sind die Unterschiede zwischen den Versionen 4 und 6. Diese erstrecken sich nicht nur auf die Adresslänge. Vielmehr findet ein Paradigmenwechsel auf vielen Ebenen statt: den Adressen, dem Protokoll und den Funktionen. Nur wer diese Unterschiede im Detail kennt, kann sein IPv6 Netz sinnvoll planen, betreiben und im Zweifelsfall die Fehler finden.

IPv6 bringt als Seminar einige spezielle Rahmenbedingungen mit sich:
- Die Teilnehmer kommen mit unterschiedlichen Vorkenntnissen zu IPv4
- Es gibt Sonderthemen, die nicht alle Teilnehmer betreffen
- In der Umsetzung des Gelernten entstehen schnell weitere Fragen

Um dem gerecht zu werden haben wir dieses Seminar in vier Teile aufgeteilt. Damit integrieren wir Videos, Präsenzschulung und Webinare in einem Seminar. Diese Aufteilung orientiert sich an den neuesten Erkenntnissen der Forschung und ermöglicht sowohl einen optimalen Lernerfolg für die Teilnehmer als auch eine Anpassung an die unterschiedlichen Anforderungen der Teilnehmer:

1. Vorbereitung
In vier Videoschulungen werden die notwendigen Grundlagen des IP Protokolls vorgestellt. So ist sichergestellt, dass bei der Präsenzveranstaltung alle Teilnehmer



denselben Stand an Vorkenntnissen haben und damit keine Zeit verloren geht, um Mechanismen zu erklären, die aus IPv4 übernommen wurden.

2. Präsenzschulung
Videos beantworten keine Fragen: Aus diesem Grund werden die zentralen Inhalte der Schulung in einer zweitägigen Präsenzveranstaltung vermittelt.

3. Spezialthemen und Vertiefung
Um das Gelernte zu wiederholen und einige Spezialthemen behandeln zu können, werden den Teilnehmern Videoschulungen zur Nachbereitung zur Verfügung gestellt, die das Gelernte wiederholen und ergänzen.

4. Webinare
Abgerundet wird die Schulung durch zwei Webinare, in denen offene Fragen geklärt und abschließende Diskussionen geführt werden.

Inhalt der Präsenzschulung
Warum (jetzt) IPv6?
- Warum die Provider mit der Umstellung bereits begonnen haben
- Warum und wo Unternehmen auf diese Umstellung reagieren müssen
- Welche Probleme bereits heute durch die Umstellung entstehen

IPv6: Das neue Protokoll
- Header: was ist neu, was ist geblieben, was fehlt
- IPv6 Header Extensions
- Alte Funktionen, neue Mechanismen am Beispiel der Fragmentierung bei IPv6

Adresskonzepte
- Aufbau und Notation der IPv6 Adresse
- Adresstypen: Lokale Adressen, Unicast, Multicast, Anycast
- Unicast-Prefixe
- Adresszuweisung
- Paradigmenwechsel: mehr als eine IPv6 Adresse pro Interface

Multicast & ICMP
- Die Ablösung der Broadcasts: Multicast
- SNMA statt ARP
- Auffinden von Routern und Nachbarn
- Multicast Listener Discovery (MLD)
- Warum ICMP an Bedeutung gewonnen hat?

Betrieb
- IPv6 Design
- DNS, ein unverzichtbares Hilfsmittel
- DHCPv6: Überflüssig oder unverzichtbar
- Interface-Anteil: welche Variante für welchen Einsatzzweck
- Dual-IP: Lösung oder Mutter aller Migrationsprobleme?

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Seminar*plus* - IPv6 Grundlagen

☐ Ich buche das Seminar*plus*
IPv6 Grundlagen
vom 16.09. - 17.09.13 in Berlin
zum Preis von € 1.790,-- netto

Buchen Sie über auch über
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Zweitthema

Verkabelung am Arbeitsplatz: Alles wie gehabt?

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Anforderungsanalyse

Bei jeder Einführung von neuen, gegebenenfalls besseren und insbesondere teureren Techniken sollte sich die Bewertung von sinnvollen und nicht sinnvollen Materialien immer am Nutzen innerhalb des erwarteten Nutzungszeitraumes orientieren. Die erwartete Nutzung muss die technische Anforderungen an die Übertragungsqualiät und den weiteren Materialqualitäten definieren, nicht die reine technische Machbarkeit oder das Marktangebot. Unter diesem Gesichtspunkt erfolgt zunächst eine kurze Anforderungsanalyse, betrachtet werden allgemeine und spezielle Anforderungen an eine Tertiärverkabelung.

Universalität

Das Ziel einer Tertiärverkabelung muss sein, dass sich Kommunikationsendgeräte am Arbeitsplatz beliebig an vorhandene passive Kommunikationsanschlüsse anschließen lassen, ohne dass ein komplexer „handwerklicher" Montagevorgang notwendig wäre. Es muss selbstverständlich ein Telefon gegen einen Drucker ausgetauscht werden können, ohne einen Elektriker oder IT-Techniker dazu heranziehen zu müssen. Daraus entsteht die Konsequenz, dass alle passiven Kommunikationsanschlüsse (die DIN/EN bezeichnet diese als Teilnehmeranschlüsse TA) eine identische Anschlusstechnik besitzen und jede am Arbeitsplatz denkbare Übertragungstechnik nutzbar macht.

Aus dieser einfachen und trivialen Forderung entsteht bereits eine erste Technologieentscheidung, nämlich eine seit vielen Jahren praktizierte Abkehr von verschiedenen Medien im Tertiärbereich. Wie sinnvoll bzw. betriebsfreundlich wäre es, sowohl Glasfaser- als auch Kupferports am Arbeitsplatz bereitzustellen und diese verschiedenen Techniken bei Änderungen der Endgerättypen bzw. deren Anschlüsse einzusetzen.

Die hohe Durchdringung der Ethernet-Techniken für (fast) jedwede IT-Kommunikation am Arbeitsplatz macht die Planung deutlich einfacher. Denn mit einer weiterhin erwarteten Dominanz des Ethernets gibt es nur noch zwei wichtige technische Aspekte, die im Rahmen der Nutzeranforderungen betrachtet werden müssen,

- die Datenrate
- die Nutzung von Power over Ethernet.

Nutzungszeitraum

Wie bereits angesprochen sollten die geforderten technischen Anforderungen bzw. Qualitäten sich unbedingt am Nutzungszeitraum einer Verkabelung orientieren. Sowohl die DIN/EN 50173 als auch ein allgemeines „Planer-Ethos" sehen die Nutzbarkeit einer Tertiärverkabelung von 10 bis 15 Jahren, besser sogar 20 Jahren vor, in der es zu möglichst wenig Nachverkabelungen und Installationsänderungen kommen darf. In der Vergangenheit zeigte sich, dass der Bedarf an Nachverkabelung eher durch eine nicht ausreichende Anzahl von geplanten Tertiäranschlüssen als durch mangelhafte Qualität der Verkabelung entstanden ist.

Dies gilt selbst bei einer Betrachtung von sehr alten Verkabelungssystemen wie z.B. die IBM-Typ-1-Verkabelung, ein Produkt der 80er-Jahre, welches heute noch in Einzelumgebungen im Einsatz ist. Eine weitere Nutzbarkeit wäre bedingt durch die hohe Qualität weiterhin denkbar gewesen, wenn diese durch systembedingte 4-Adrigkeit nur 100 Mbit/s übertragen könnte.

Andererseits muss man aber auch ein Gegenbeispiel aufzeigen, bei dem für bestimmte Übertragungsqualitäten und damit prognostizierter Nutzbarkeitszeitraum sich dieser nicht erfüllte: Die Ende der 90er bzw. Anfang 2000er eingeführte Übertragungsqualität der Klasse E (Achtung: nicht Klasse E_A) brachte überhaupt keinen nutzbaren Vorteil im Vergleich zur Klasse D. Bei Installationen mit dieser 250MHz-Tertiärverkabelung, insbesondere im Rechenzentrumsumfeld, muss möglicherweise im Nutzbarkeitszeitraum mit Einschränkungen gerechnet werden.

Installations- und Betriebsfreundlichkeit

Selbst wenn in einem langen Nutzbarkeitszeitraum alle benötigten Übertragungstechniken im Tertiärbereich verwendet werden, können die verschiedenen Verkabelungen unterschiedliche Vor- und Nachteile bei der Installation und auch beim späteren Betrieb haben. Die Installationsfreundlichkeit spielt aus der Sichtweise des Nutzers zunächst eine untergeordnete Rolle (dazu später mehr), sie ist relevant für den Planer der Erstinstallation, dort verursacht sie höhere Investitionskosten.

In Zusammenhang mit der Betriebsfreundlichkeit einer Kommunikationsverkabelung sind Anforderungen zu nennen, die zum einen in Zusammenhang mit der Fehleranfälligkeit und der Fehlerbehebbarkeit zu sehen sind. Beispielsweise ist eine Anschlussschnur (bestehend aus Anschlusskabel und Stecker) zwar nicht Gegenstand der festen Verkabelung, hat aber erfahrungsgemäß einen großen Einfluss auf die Übertragungsqualität der zu nutzenden Strecke und damit deren Verfügbarkeit. Auf der anderen Seite kommt neben der Betrachtung dieser Fehleranfälligkeit auch eine Bewertung der Änderungsflexibilität bei Umzügen oder Nutzungsänderungen hinzu. Wie einfach lassen sich z.B. in Gebäuden mit vermieteten Büroflächen Mieterwechsel durchführen, ohne dass mehr-

fach eine vollständige Neuverkabelung notwendig wird, weil der Nachfolgemieter andere Anforderungen an die Tertiärverkabelung, z.B. durch veränderte Möblierung, stellt.

Kostenminimierung

Bei allen technischen Anforderungen bleibt natürlich am Ende auch die Bewertung der Kosten, die zur Einrichtung der Infrastruktur aufzuwenden sind. Die Notwendigkeit ein bestimmtes Maximalbudget einzuhalten wird in vielen Fällen die entscheidende Anforderung sein und eine Analyse der zu erwartenden Kosten bzw. der damit verbundenen Optimierungspotenziale muss viele Aspekte berücksichtigen. Installationskosten lassen sich relativ einfach und genau mit Hilfe von Kostenschätzungen ermitteln, dagegen ist die Schätzung von Betriebskosten mit sehr vielen spekulativen Annahmen verbunden.

Nutzbare Datenrate

Den meisten Lesern wird bekannt sein, dass für die Ethernet-Technologien derzeit IEEE-Standards bis zu einer maximalen Datenrate von 100 Gbit/s bestehen. Die Übertragungstechniken für 40 Gbit/s und 100 Gbit/s lassen sich (noch) nicht mit Twisted Pair realisieren. Da davon auszugehen ist, dass die deutlich größere Menge an Tertiärinstallationen mit dem Medium Twisted Pair realisiert worden ist, kann die Nutzbarkeit dieser beiden Datenraten für den Tertiärbereich ausgeschlossen werden. Aktuell läuft eine sehr intensive Diskussion, ob 40 Gbit/s möglicherweise doch über Twisted Pair möglich sein könnte, die Nutznießer einer derartigen Innovation dürften wohl eher im Rechenzentrumsbereich gesehen werden. Damit stehen für den Tertiärbereich Datenraten bis zu 10 Gbit/s mit einer brauchbaren Reichweite von ca. 100 m zur Verfügung. (siehe Abbildung 1)

Umfragen des Autors im Rahmen seiner Seminartätigkeit und auch im Rahmen seiner Projektierungen ergeben, dass nur in ca. 50% der Netzwerkumgebungen eine Datenrate von mindestens 100 Mbit/s flächendeckend, also an jedem Arbeitsplatz, wirklich benötigt wird (es steht natürlich fast überall 100 Mbit/s zur Verfügung). Damit lässt sich die Aussage treffen, dass eine Datenrate von 1 Gbit/s für die nächsten 10 bis 15 Jahre als „mehr als ausreichend“ zu sehen ist. Was ist dazu notwendig?

Die im Zusammenhang mit 1 Gbit/s zu berücksichtigende IEEE-Spezifikation 802.3ab stellt keine wirklich „Herausforderung“ an die Verkabelungskomponenten dar, es reicht eine Verkabelung in der Güte Klasse D mit Kategorie-5-Komponenten nach aktueller EN 50173; Klasse E oder mehr ist nicht notwendig. Erfahrungsgemäß ist davon auszugehen, dass nahezu alle 8-adrigen Twisted-Pair-Verkabelungen in Deutschland Gigabit-tauglich sind.

IEEE-Standard	Bezeichnung	Jahr	Datenrate	Kabel
802.3j	10Base-T	1990	10 MBit/s	TP-Kabel (RJ-45)
802.3j	10Base-FL	1992	10 MBit/s	Glasfaserkabel
802.3u	100Base-TX	1995	100 MBit/s	TP-Kabel (RJ-45)
802.3u	100Base-FX	1995	100 MBit/s	Glasfaserkabel
802.3z	1000Base-SX 1000Base-LX	1998	1 GBit/s	Glasfaserkabel
802.3ab	1000Base-T	1999	1 GBit/s	TP-Kabel (RJ-45)
802.3an	10GBase-T	2006	10 GBit/s	TP-Kabel (RJ-45)

Abbildung 1: Übersicht der im Tertiärbereich relevanten Ethernet-Techniken

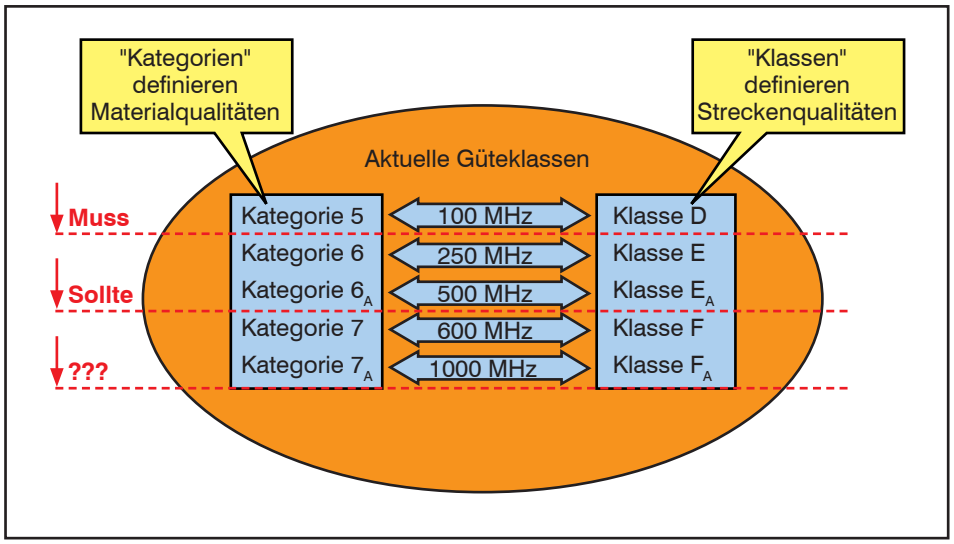


Abbildung 2: Güteklassen bei Kupfer

Gerade im Umfeld von Planungen im deutschen Umfeld reicht den meisten Planern aber eine ausschließliche Einforderung der Klasse D nicht aus, hier herrscht (im Unterschied zum Ausland) ein sehr ausgeprägtes „Reservebewusstsein“ mit dem Ziel, kein Risiko bezüglich des Nutzbarkeitszeitraumes einzugehen und damit jede denkbare Datenrate im Tertiärbereich sicherstellen zu müssen. Wie oben bereits ausgeführt würde das zu einer Verkabelung mit einer nutzbaren Datenrate von 10 Gbit/s am Arbeitsplatz führen. Daraus leitet sich eine Forderung nach Nutzbarkeit der 10GBase-T-Technik gemäß IEEE 802.3an ab und dies wiederum führt zu einer Forderung nach Klasse E_A (oder besser) im Tertiärbereich, Klasse E bringt hier gar nichts. Es ist einem Umstand zu verdanken, dass in allen aktuellen Planungen von Gebäudeverkabelungen diese Klasse E_A vorgesehen wird: Der Kostenunterschied zwischen einer Klasse D/E-Verkabelung und einer Klasse E_A-Verkabelung ist so gering, dass sich ein Verzicht auf die niedrigere Qualität nicht lohnt. Teilweise ist es schwieriger auf dem Markt Kategorie 5-Systeme oder Kabel zu bekommen als Kategorie 6_A-Komponenten. (siehe Abbildung 2)

Bleibt die Frage, ob eine weitere Verbesserung der Streckenqualität durch Schaffung von noch größeren Systemreserven zu einer besseren Funktionalität der Strecke und damit zu einem längeren Nutzbarkeitszeitraum führt. Eine höhere Datenrate als 10 Gbit/s ist zum aktuellen Zeitpunkt nicht möglich, falls dies überhaupt jemals am Arbeitsplatz von Nutzen sein würde, aber wie sieht es mit völlig anderen Techniken aus?

Lange Zeit wurde als Vorteil der nächst höheren Leistungsklasse F und F_A das Cable-Sharing angepriesen, denn mit Anschlusstechniken der Kategorie 7 bzw. 7_A lässt sich dies besonders „verlustarm“ nutzen. Da angesichts der 8-adri-

Verkabelung am Arbeitsplatz: Alles wie gehabt?

gen Gigabit-Techniken wohl kaum ein Bedarf nach Cable-Sharing besteht und auch herkömmliche Klasse E/E_A-Systeme diese Technik unterstützen, stellt das keinen Vorteil der 600/1000-MHz-Techniken dar.

Ähnliches gilt für Breitbandübertragungen über Twisted-Pair, die zu Ende der 90er-Jahre bevorzugt über Klasse F eingesetzt wurde. Auch diese Art von Übertragungstechnik kommt mit Verkabelungen der Klasse E oder E_A sehr gut aus, passende Balun-Techniken werden z.B. durch Dätwyler hergestellt.

Auch hier gilt: Würde eine Installation der Klasse F/F_A annähernd kostenneutral zur Klasse E_A sein, so spräche wenig dagegen, dies in neuen Gebäudeverkabelungen so vorzusehen. Die Kosten im Bereich der Anschlusstechnik liegen aber sowohl beim Material als auch bei der handwerklichen Dienstleistung immer noch höher, so dass eine Entscheidung für ein technisch besseres System ohne erkennbaren Mehrnutzen gut zu überlegen ist.

Somit kommt der Autor zum Ergebnis, dass ein Bedarf und damit eine Notwendigkeit nach „mehr als Klasse E_A“ im Tertiärbereich nicht ersichtlich ist oder sich in den nächsten 10-15 Jahren abzeichnen wird. Stimmt die in Fachkreisen genannte Angabe, dass nur 1% der weltweiten Installationen eine Klasse-F-Qualität haben, stellt sich ohnehin die Frage, welcher Hersteller von Switches ein Gerät oder Interface-Karten entwickeln wird, welches Kupferports mit einer Kategorie-7- bzw. Klasse-F-Qualität oder besser benötigt.

Power over Ethernet

Neben der Bereitstellung einer hohen Datenrate bildet die Möglichkeit, Strom über ein Datenkabel übertragen zu können, die zweite spezielle Anforderung, die näher zu betrachten ist. Dabei ist zunächst zu entscheiden, welche maximale Leistung am Endgerät (Power Device) benötigt wird. Derzeit stehen zur Verfügung:

- Empfangsleistung am Verbraucher bis ca. 13 Watt nach IEEE 802.3af
- Empfangsleistung am Verbraucher bis ca. 22 Watt nach IEEE 802.3at

Überwiegen zum aktuellen Zeitpunkt bei weitem die Geräte, die mit der kleineren Leistung auskommen, können muss natürlich bei einer 10-15-jährigen Nutzungsdauer der Tertiärverkabelung angenommen werden, dass sich dies ändern könnte. Die beiden Techniken unterscheiden sich und dies hat einen Einfluss auf die Nutzbarkeit der Verkabelung, insbesondere der Altverkabelungen.

Abbildung 3 zeigt das Grundprinzip von IEEE 802.3af. Wichtig sind folgende Details:

Es werden 2 Alternativen spezifiziert, die in 3 denkbaren Varianten genutzt werden können. Bei Alternative A werden die Paare 1 und 4 genutzt (= PINs 1/2 & 3/6). Die Paare 2 und 3 (= PINs 4/5 und 7/8) werden nicht benötigt. Damit kann Alternative A bei einer 4-adrigen Verkabelung genutzt werden, gelegentliche Behauptungen „PoE geht nur mit einer 8-adrigen Verkabelung“ sind falsch. Alternative A lässt sich bei Nutzung der Datenrate 1 Gbit/s verwenden (was dann natürlich 8-Adrigkeit voraussetzt). Der Einsatz von externen MidSpan-Komponenten ist nicht möglich und es muss ein Switch mit PoE-Funktionalität vorhanden sein.

Bei Alternative B erfolgt die Stromübertragung über die Paare 2 und 3. Da bei Ethernet immer mindestens die Paare 1 und 4 zur Datenübertragung genutzt werden, erfordert Alternative B damit immer eine 8-adrige Verkabelung. Etwas „verwirrend“ ist, dass kein mit PoE nach Variante B Gigabit möglich ist (obwohl 8 Adern für PoE gefordert werden), dafür können MidSpan-Geräte eingesetzt werden.

Für beide Varianten reicht eine Verkabelung der Klasse C (bzw. Kategorie 3) aus, was somit durch die meisten IT-Verkabelungen sichergestellt wird. Auf den Punkt gebracht bedeutet dies, dass alle 4-adrigen Verkabelungen mit Alternative A arbeiten können, dies nur unter Einsatz von Switches mit PoE. 8-Adrigkeit dagegen bietet die gesamte Funktionalität.

In Abbildung 4 wird das Grundprinzip von IEEE 802.3at dargestellt, wichtig sind folgende Details:

IEEE802.3at übernimmt die alten Varianten (= ein Switch mit IEEE802.3at-Unterstützung kann auch Endgeräte mit IEEE802.3af-Technik versorgen) und ergänzt um neue. Es wurden zusätzlich 2 neue Alternativen spezifiziert, die in 4 denkbaren Varianten genutzt werden können. PoE ist grundsätzlich nur mit einer 8-adrigen Verkabelung möglich, 1000Base-T und MidSpan (auch mit 1000BaseT) geht bei beiden Alternativen.

Im nachfolgenden und letzten Teil des Artikels wird ein Aspekt beleuchtet, der weniger geprägt ist von nachrichten- oder elektrotechnischen Kriterien, vielmehr geht es um die möglichen betrieblichen Vorteile eines Einsatzes von Sammelpunkten (Consolidation Points),

Flexibilität bei Nutzungsänderungen am Arbeitsplatz

Immer dann, wenn ein neues Gebäude mit umfangreichen Bürobereichen geplant und gebaut werden soll, ergibt sich für die IT-Verkabelung eine besondere Situation, die nicht zu vergleichen ist mit Standard-Elektroverkabelungen am Arbeitsplatz. Die Besonderheit liegt darin, dass im Unterschied zur Elektroverkabelung in der Regel von einem zentralen Etagenverteiler

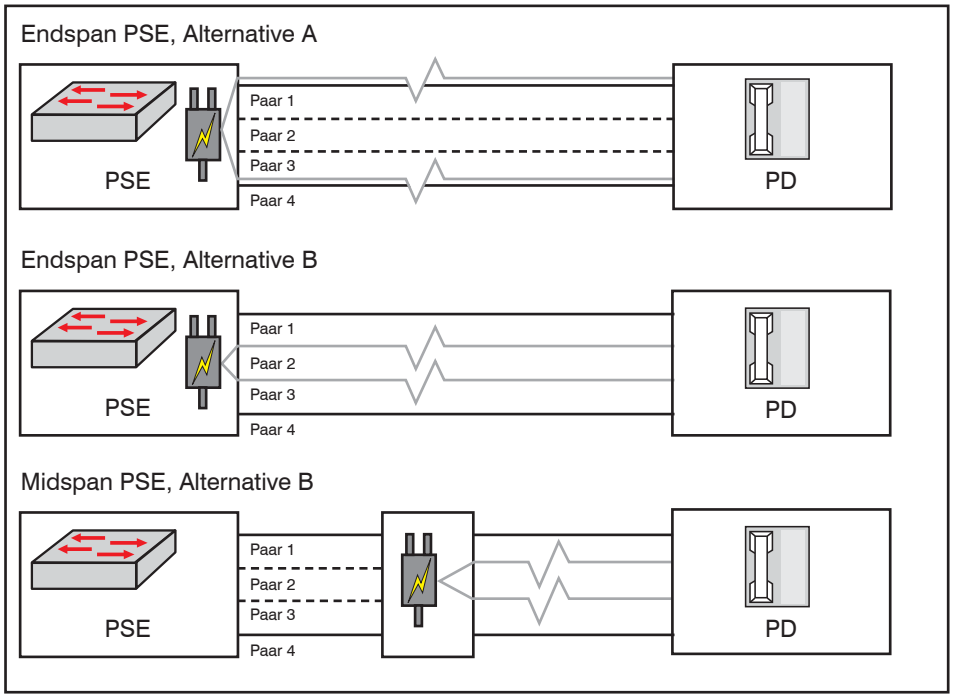


Abbildung 3: Power over Ethernet nach Variante „IEEE802.3af“

Verkabelung am Arbeitsplatz: Alles wie gehabt?

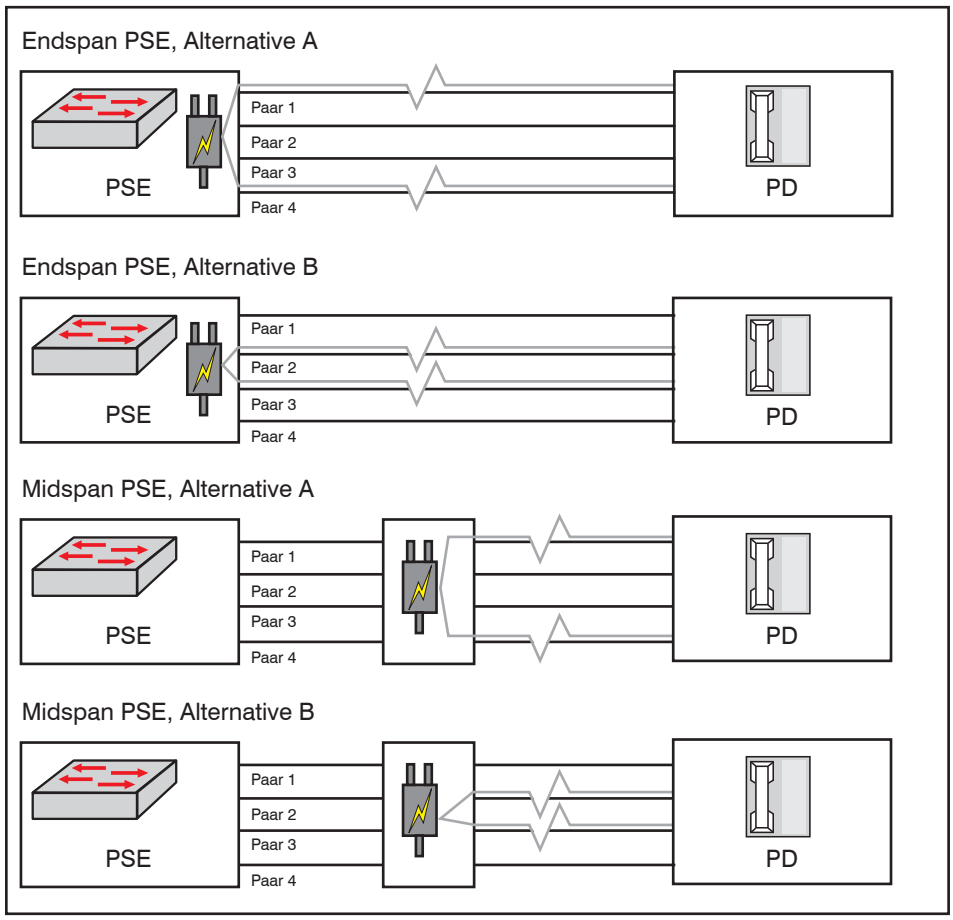


Abbildung 4: Power over Ethernet nach Variante „IEEE802.3at“

aus mehrere, einzelne Kabel zu einem IT-Arbeitsplatz geführt werden müssen. Die EN 50173-1 bzw. EN 50173-2 selbst sieht eine minimale Anzahl von 2 Datenkabel pro Arbeitsplatz vor. In der Praxis zeigt sich aber, dass bei einer Nutzung der „Datenkabel“ durch direkt angeschlossene Telefonapparate (klassische Telefone oder auch VoIP-Telefone), mindestens 3 Kabel vorzusehen sind. Berücksichtigt man optionale weitere Zusatzdienste wie z.B. Druckeranschlüsse am Büroarbeitsplatz, so stellt eine Anzahl von 3 „Datenkabeln“ pro IT-Arbeitsplatz eine sinnvolle Größe dar. Strom- und Datenleitungen sollen nach Möglichkeit nicht sichtbar zu den Datenendgeräten geführt werden. Bei der Stromversorgung beschränkt sich dies häufig auf eine einzige Zuleitung pro Tisch, im Datenbereich müssen jedoch alle Datenkabel einzeln zum Tisch geführt werden. (siehe Abbildung 5)

Zur Führung der Strom/Datenkabel zu den IT-Arbeitsplätzen stehen zwei Hauptverfahrensweisen zur Verfügung, zunächst wird das Grundprinzip einer Kabelführung mit sichtbaren Kabelführungssystemen erläutert. Hierbei werden Leitungsführungskanäle oder Geräteeinbaukanäle im sichtbaren Bereich (zumeist unterhalb der Fenster) montiert, die in der Regel sowohl für Strom- als auch für Datenkabel und dazugehörende Anschlusseinheiten genutzt werden. Der Vorteil dieser Lösung liegt in der einfachen Zugänglichkeit bei Nachverkabelungen oder Reparaturen (Voraussetzung: ausreichende Kapazität wurde vorgesehen). Diese Lösung hat jedoch zwei entscheidende Nachteile:

1. Durch die Sichtbarkeit der Kanäle werden die gestalterischen Möglichkeiten des Architekten insbesondere im Fensterbereich eingeschränkt (z.B. keine bis zum Boden reichende Glasfenster).

2. Die an der Anschlussdose (montiert im Fensterbankkanal) angeschlossen Anschlussschnüre müssen bis zum IT-Endgerät geführt werden. Befindet sich der Standort des Endgerätes relativ weit entfernt vom Fenster, so ist mit größeren Längen störender Anschlusskabel zu rechnen. Tische mit Arbeitsplätzen weit entfernt vom Fenster lassen sich nicht benutzerfreundlich anschließen oder es müssen weitere Kanäle auf den Zwischenwänden vorgesehen werden. Umzüge bzw. Veränderungen der Tischpositionen verschlechtern häufig die Situation.

Abbildung 5: Kabelchaos am Arbeitsplatz

Die Raummöblierung muss sich also sehr eng an das Kabelführungssystem orientieren und schränkt die Flexibilität erheblich ein, aus diesem Grunde kommen derartige sichtbare Kabelführungssysteme in Neubauten immer seltener zum Einsatz.

Die zweite Verfahrensweise mit einer versteckten Kabelführung sieht wie folgt aus. Zwischendecken, Doppelboden und Hohlraumboden ermöglichen eine nichtsichtbare Kabelführung. Die Zwischendecke scheidet jedoch meistens als nutzbare Variante aus, weil mit komplizierten Lösungen die Verkabelung von der Zwischendecke hinab zu den Arbeitstischen geführt werden müsste. Die Lösung mit Doppelboden und Unterflurtanks hat folgende Vor- und Nachteile:

1. Sie erlaubt in Grenzen eine beliebige Kabelführung und beliebige Positionierung von Anschlusseinheiten mit Datenanschlüssen.

2. Vom Unterflurtank müssen Anschlussschnüre zum Arbeitstisch geführt werden. Befindet sich der Tisch unmittelbar in der Nähe des Unterflurtanks, so ist der Anteil an sichtbaren und störenden Kabeln gering, Stolpermöglichkeiten sind nur wenig vorhanden. Ändert sich jedoch bei Einzug in das Gebäude oder bei Mitarbeiterumzügen die Tischposition, so besteht die Gefahr, dass sich der Unterflurtank in einer „großen“ Entfernung zum Tisch befindet. Daraus resultieren sehr häufig wieder „freifliegende Kabellängen“ zwischen 0,5 und 1,5 m oder auch Blockierungen des Zugangs zum Bodentank.

Erfahrungen zeigen, dass diese „klassische“ Lösung bereits bei Einzug in das Gebäude sehr benutzerunfreundlich ist und im Laufe der Jahre zur Unzufriedenheit der Mitarbeiter (Zwang zur starren Möblierung) und zu defekten Datenleitungen führt, die z.B. durch typisches „Überrollen“ mit Schreibtischstühlen verursacht werden.

Verkabelung am Arbeitsplatz: Alles wie gehabt?

Grundprinzip des Sammelpunktes

Der Einsatz von Sammelpunkten (nachfolgend mit SP abgekürzt) bzw. Consolidation Points soll gemäß EN 50173-1 dem Nutzer die Möglichkeit geben, längere Anschlussschnüre vorzusehen, diese sind ohne SP auf üblicherweise maximal 5 Meter begrenzt. Der SP stellt einen Verteilerpunkt dar, der keine aktiven Komponenten beinhaltet, sondern lediglich Buchsen, welche die dauerhaft festinstallierten Tertiärkabel (nach EN „Stammkabel“ genannt) abschließen. In die Buchsen werden Stecker gesteckt, die an nicht dauerhaft verlegte Kabel angeschlossen wurden (Sammelpunkt-Kabel), diese Kabel werden zu einer Anschlussdose bzw. der darin befindlichen Anschlussbuchse (Teilnehmeranschlusseinheit TA) geführt. Damit sind für den Nutzer die SPe ein „unsichtbarer“ Teil der IT-Verkabelung, der im Regelfall nicht zum Betrieb zugänglich sein muss; erst bei größeren Umzügen mit Veränderungen der TA ist eine Zugänglichkeit erforderlich. (siehe Abbildungen 6 und 7)

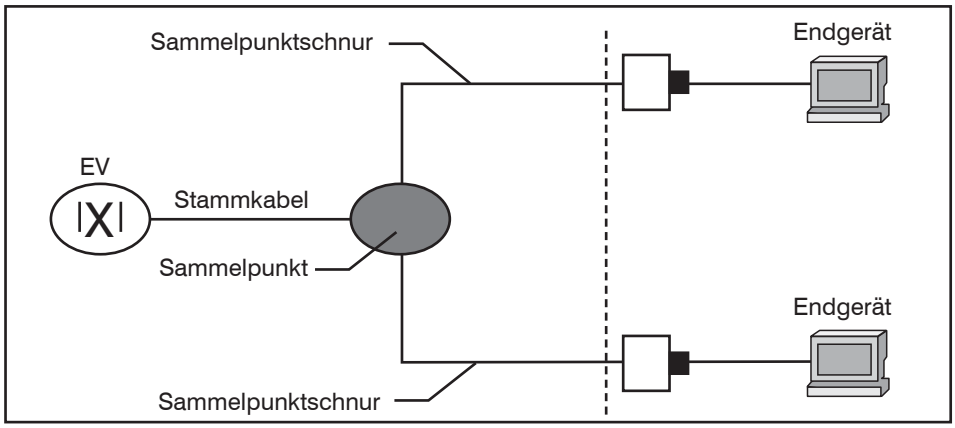


Abbildung 6: Teilelemente Sammelpunkt nach EN 50173

Der Nutzen des Sammelpunktes wird anhand der beiden Abbildungen 8 und 9 ersichtlich. Die beiden Abbildungen zeigen eine Beispieletage mit Standardbüros links und rechts neben einem Flur. Der Flur besitzt einen leicht zu öffnenden Doppelboden und im Bürobereich steht ein Hohlraumboden oder Doppelboden zur Verfügung, beides sind wesentliche notwendige Rahmenbedingungen zum effektiven Einsatz von Sammelpunkten. Die jeweils unten dargestellte Etage jedes Doppelbildes zeigt die Arbeitsplatzbelegung und damit zusammenhängende Verkabelung zum Einzug der Etage, das darüber liegende Bild dagegen die Arbeitsplätze z.B. nach einem später erfolgten Abteilungs- oder Mieterwechsel inklusive einer Änderung der Raumaufteilungen und Größen.

In einer Installation nach Abbildung 8 würde diese Änderungen zwangsläufig eine Nachverkabelung für den gesamten Bereich zwischen dem im Bild nicht dargestellten Etagenverteiler und den Büros notwendig machen. Um die neue Anzahl von 88 Twisted-Pair-Leitungen bereitzustellen müssten 8 Strecken über größere Distanzen nachgezogen werden. Es wäre mit umfangreichen Öffnungen der Kabelwege über eine größere Strecke wie auch Brandschotts o.ä. zu rechnen.

Bei Abbildung 9 dagegen wurden „vorsorglich“ Sammelpunkte im Doppelboden des Flurs montiert, die sich nicht an der ersten Raumplanung orientierten, sondern an der potenziell möglichen Anzahl von Arbeitsplätzen pro Flächeneinheit (Positionierung der SP in einem vorher zu bestimmenden Raster). Dazu wurden diese mit insgesamt 96 Stammkabel versorgt, also 16 mehr als beim Erstausbau von Variante aus Abbildung 8. Beim Ersteinzug wur-

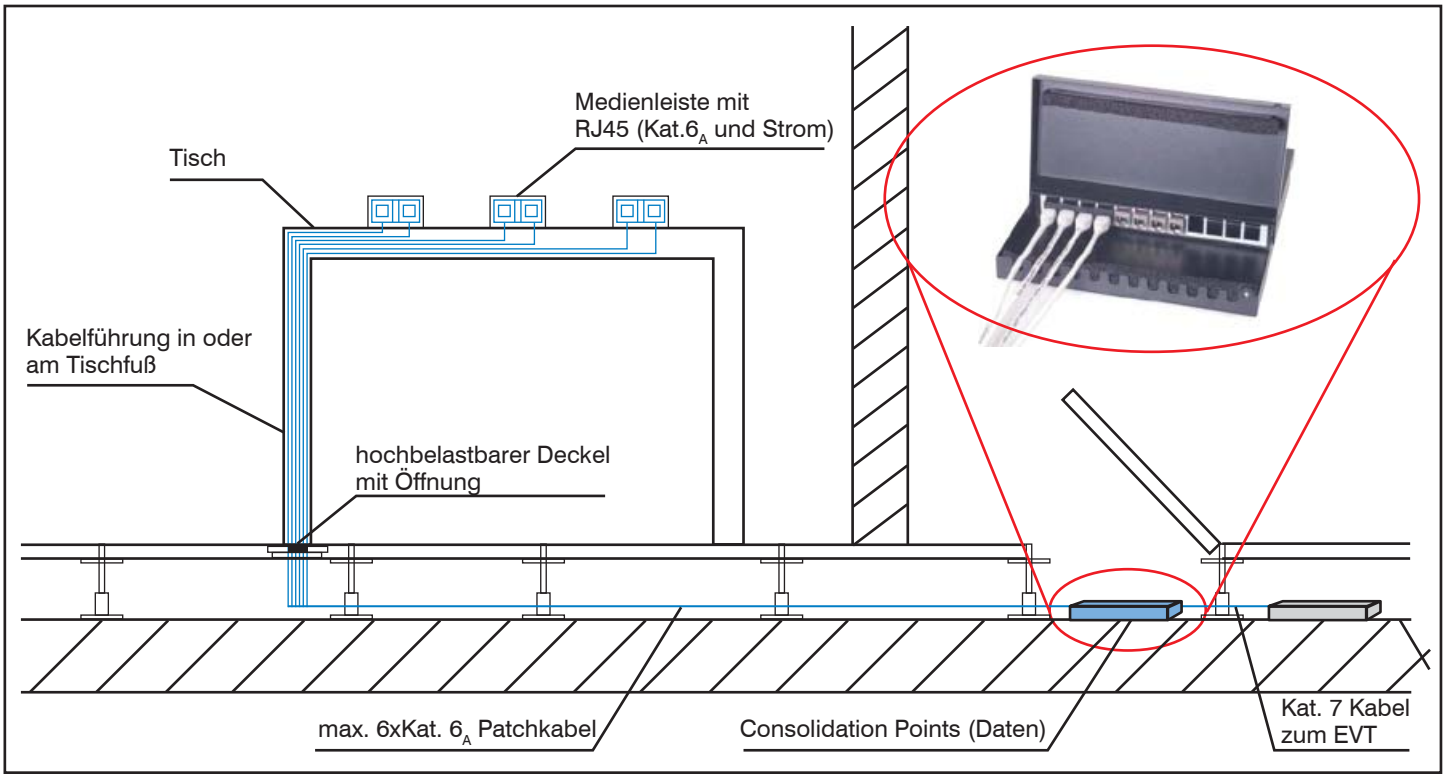


Abbildung 7: Detaildarstellung Lage und Anschlussprinzip Sammelpunkt

Verkabelung am Arbeitsplatz: Alles wie gehabt?

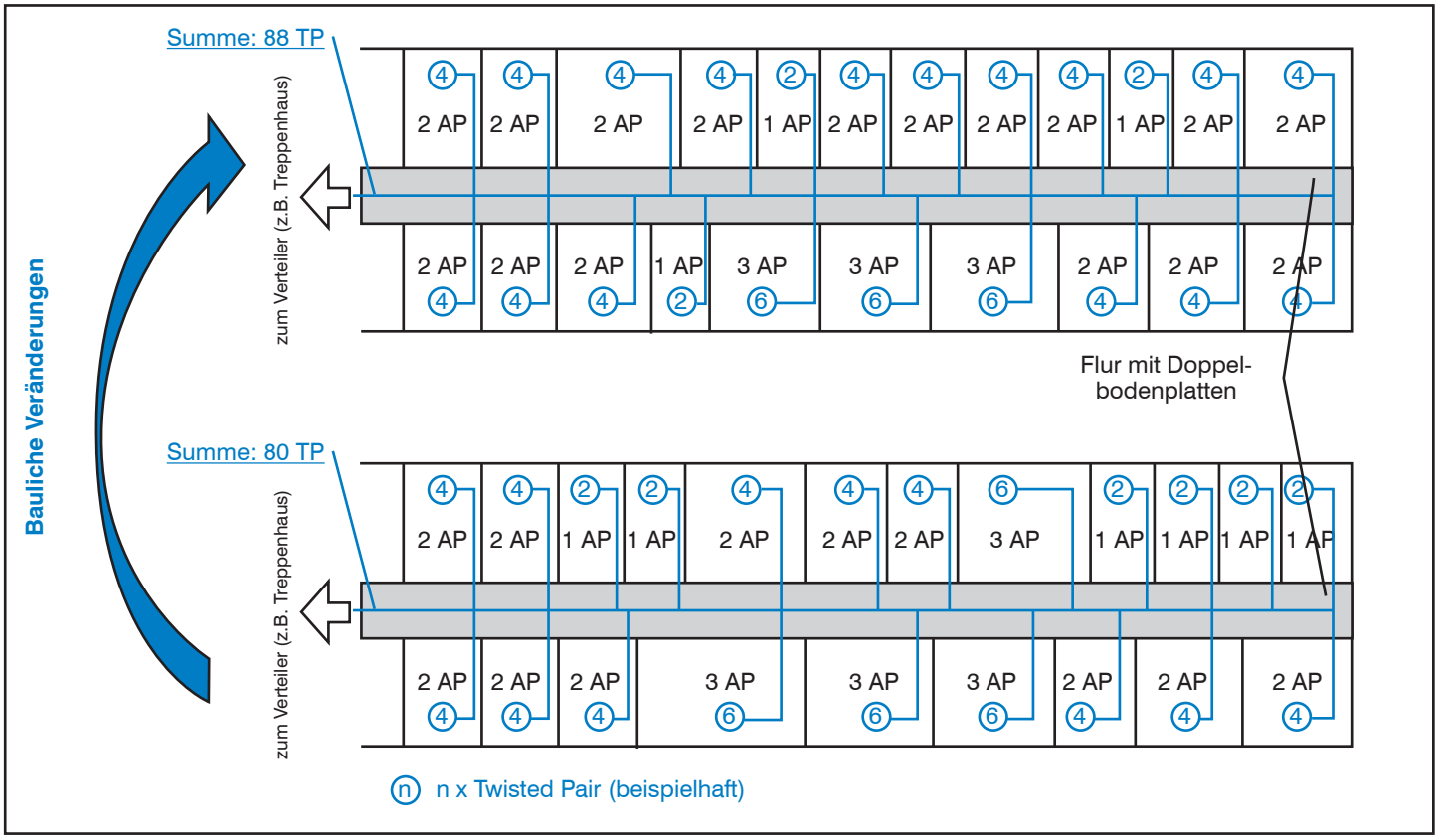


Abbildung 8: Projektbeispiel, Tertiärverkabelung klassisch ohne Sammelpunkt

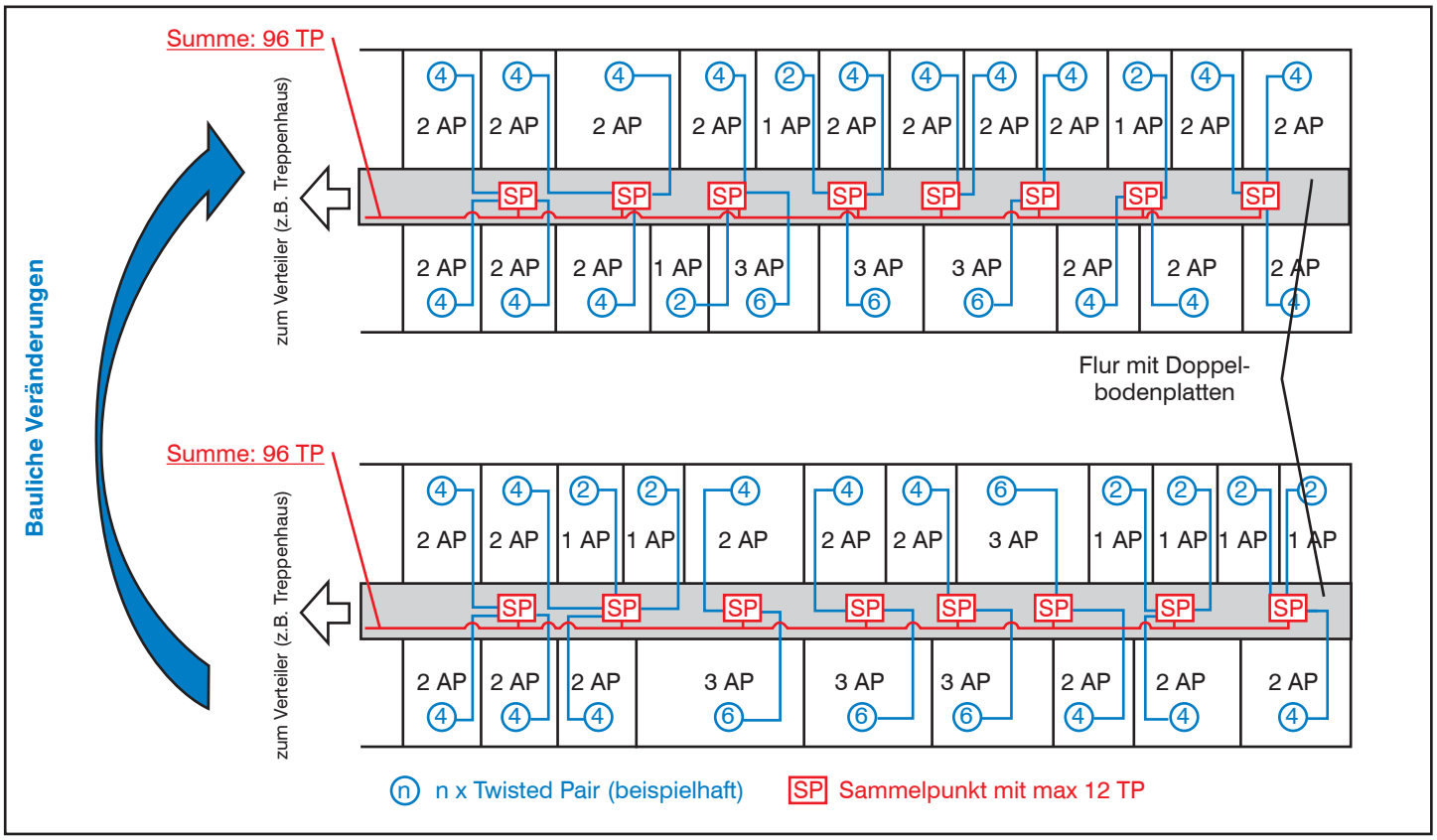


Abbildung 9: Projektbeispiel, Tertiärverkabelung mit Sammelpunkt

de nur ein Teil der in den SP bereitgestellten Ports beschaltet. Nach dem Umzug wurde diese Beschaltung geändert und es mussten nur die Sammelpunktschnüre umverlegt oder neuverlegt werden, was deutlich geringere Installationsarbeiten notwendig macht, insbesondere „unangenehme“ Maßnahmen wie Brandschott Öffnen/Schließen können vermieden werden. Deutlich wird aber auch, dass es bei der Variante mit Sammelpunkten nicht zu einer Kostenersparnis kommt (96 Leitungen im Vergleich zu 88 Leitungen), es wird „nur“ ein Vorteil im Punkt Flexibilität und Betriebsfreundlichkeit erzielt, der aber natürlich letztendlich Umzugskosten – gerade bei häufigen Umzügen – reduzieren kann.

Dieses in der Theorie sehr ansprechende Prinzip wird gerne von Bauherren eines Gebäudes eingesetzt, welche die Büroflächen selber nicht nutzen, sondern vermieten. Der „Vermieter“ stellt die gesamte Infrastruktur bis inklusive des SP zur Verfügung, die Sammelpunktschnur inkl. der Dosen mit den Anschlüssen sind dann vom Mieter beizusteuern. Leider zeigen die Erfahrungen, dass der Mieter nur unter ganz bestimmten Voraussetzungen mit dieser, grundsätzlich durchaus sinnvollen Technik „glücklich“ werden wird:

1. Der Mieter muss sich frühzeitig Gedanken machen, wie sich Umzüge auf die Nutzbarkeit der vom Vermieter bereitgestellten Verkabelung auswirken. Häufig gehen nämlich die Nachverkabelungen zu Lasten des Mieters. Beispielsweise werden häufig vor Einzug der Räumlichkeiten Bereiche mit niedriger Anzahl von Arbeitsplätzen (z.B. in Besprechungsräumen) mit wenigen oder gar keinen Sammelpunkten ausgestattet, bei Nutzung dieser Besprechungsräume als Büros fehlen dann SPe.

2. Es muss eine gute Zugänglichkeit des Bodens mit den Sammelpunkten sichergestellt sein. Dabei müssen die Bodenbeläge auf dem Doppelboden wie Teppich o.ä. sehr hochwertig sein, sonst wird ein häufiges Öffnen des Bodens optische Spuren hinterlassen.

3. In den Büros sollte auch ein Doppelboden bestehend aus zu öffnenden Doppelbodenplatten sein, meist wird aber aus Kostengründen hier ein Hohlraumboden vorgesehen. Dieser unterscheidet sich zum Doppelboden primär darin, dass er nicht zu öffnen ist. Demzufolge müssen bei Änderungen der Möblierung (z.B. durch Umzüge) neue Löcher in den Boden gebohrt werden, was bei hoher Umzugsrate zu sehr merkwürdigen „Bodenperforierungen“ führen kann. Bei einem Doppelboden mit wechselbaren Bodenplatten kann man die Platte mit dem Loch tauschen.

4. Bei der Planung der Anzahl und Lage von SPen ist die Festlegung der Reichweite des SPs zwischen SP und Anschlussdose (bzw. Medienleiste) von großer Bedeutung. In jedem Bereich der Etage müssen die SPe so geplant werden, dass die denkbaren IT-Arbeitsplätze innerhalb dieser Entfernung erreichbar sind. Dabei ist zu berücksichtigen, dass eine Verlegung der Sammelpunktschnur zwischen SP und TA in der Regel nicht auf dem kürzesten Wege erfolgt, sondern auf einem im Installationsbereich üblichen orthogonalen Weg.

5. Es sollten sich frühzeitig dazu Gedanken gemacht werden, wie diese Verkabelung einzumessen ist, nur die Strecke zwischen Rangierfeld und Sammelpunkt oder mit der Sammelpunktschnur? Wer ist verantwortlich bei fehlerhaften Gesamtstrecken?

6. Die Einrichtung von zusätzlichen Elektrosammelpunkten hat zum Teil zu unangenehmen Projekterfahrungen geführt, diese Kombination und vor allem die technische Umsetzung sollte gut überdacht werden.

Und wie steht es mit Glasfaser am Arbeitsplatz?

Gerade im Zusammenhang mit der Einführung von VoIP bzw. der damit notwendigen Verwendung von Power over Ethernet stellen sich viele Nutzer von „Fiber to the Desk“ oder „Fiber to the Office“ die Frage nach weiteren Investitionen in diese Technik. Nach Einschätzung des Autors gibt es nur in sehr seltenen Fällen Rahmenbedingungen, die eine Aufrechterhaltung dieser Technik im Tertiärbereich notwendig machen. In den meisten Fällen ist eine komplette Neuverkabelung mit Twisted Pair sowohl die technisch flexiblere als auch die kostengünstigere Lösung. Selbst unter Annahme von schlechten Rahmenbedingungen für die Kupferlösung und guten Rahmenbedingungen für die Glasfaserlösung wird diese Pauschalempfehlung häufig Gültigkeit behalten. Trotzdem wird angeraten, für jeden einzelnen Fall eine Analyse der Anforderungen und Rahmenbedingungen durchzuführen und erst danach mit Hilfe eines technischen und wirtschaftlichen Vergleichs eine Entscheidung zu treffen.

Vollständiger Wegfall der Tertiärverkabelung durch WLAN?

Die Standards IEEE802.11ad oder IEEE802.11ac machen es möglich, mehr als 1 Gbit/s lassen sich bis zum Endgerät ohne Kabel bringen, ist damit das Ende der Tertiärverkabelung eingeläutet? Wie der Artikel von Dr. Wetzlar im Netzwerk-Insider 11/2012 deutlich macht, lassen sich hohe funkbasierende Datenraten und zuverlässige Übertragung über „größere“ Distanzen nur schwer in Übereinklang bringen, derartige Datenraten werden wahrscheinlich nur punktuell verfügbar sein. Damit stellt ein Access-Point Datenraten von mehr als 1 Gbit/s (Brutto!) nur in einem Bereich mit Standard-Raumgröße zur Verfügung, der Access-Point würde lediglich die Geräteanschlussverkabelung sprich die „Patchkabel“ ersetzen, er stellt somit eine Art „Spot-Access-Point“ dar. Selbst für diese Access-Points muss eine Verkabelung vorgesehen werden:

Ein Spot-Access-Point pro Raum müsste geplant werden, das führt zu 1 Twisted-Pair-Kabel pro Raum. Soll weiterhin eine Sprachkommunikation über Festapparate möglich sein oder soll eine Redundanz geschaffen werden für den Fall, dass ein Link ausfällt, wird man ein zweites Kabel pro Raum vorsehen. Erkennbar wird, es werden weiterhin sehr viele TP-Kabel notwendig sein. Wie wahrscheinlich ist unter diesen Bedingungen der der Wegfall der Tertiärverkabelung?

Fazit

Die meisten modernen, aber auch älteren Tertiärverkabelungen haben eine Leistungsfähigkeit, welche die Anforderungen der auf diesen Strecken eingesetzten Endgeräte bei weitem erfüllen. Ein Bedarf nach wesentlichen Innovationen für diesen Bereich der anwendungsneutralen Kommunikationsverkabelung ist aus Sicht des Autors derzeit nicht ersichtlich. Jede neue Gebäudeverkabelung, die eine Klasse-E_A-Lösung sicherstellt, liefert am Arbeitsplatz Rechenzentrumsqualität und sollte somit mehr als ausreichend sein. Teilt man diese Prognose nicht, so kann eine Kombination von Kategorie-$7/7_A$-Installationskabel und Kategorie-6_A-Anschlusstechnik eine Möglichkeit darstellen, ein einfaches „Upgrade“ der Verkabelung durchzuführen, ohne dass man von einer kompletten Neuverkabelung ausgehen muss. Der „Sammelpunkt“ kann bei entsprechender Planung und unter bestimmten Rahmenbedingungen durchaus ein Element sein, welches eine Anpassung der Kommunikationsverkabelung bei hohen Umzugsraten oder Möblierungsänderungen einfacher macht. Der Zeitpunkt, wo funkbasierende Übertragungstechniken eine Tertiärverkabelung vollkommen ablösen werden, ist weiterhin noch nicht erkennbar, deshalb werden auch weiterhin in neuen Bürogebäuden Planungen von Tertiärverkabelungen notwendig sein.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger, 09.09. - 13.09.13 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 09.09. - 11.09.13 in Bonn

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance"-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam" zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice"-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter" Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 16.09. - 18.09.13 in Berlin

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco und Siemens aber auch des Newcomers Microsoft.

Preis: € 1.890,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 16.09. - 18.09.13 in Berlin

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 16.09. - 18.09.13 in Berlin

Dieses Seminar liefert einen umfassenden und zugleich detaillierten Einblick in die aktuellen Virtualisierungstechnologien der marktführenden Anbieter. Vom Server über das Netzwerk bis zum Speicher und schließlich auch zum Client werden die Möglichkeiten und Grenzen der Virtualisierungslösungen analysiert. Dabei bleiben auch Sicherheitsaspekte nicht unberücksichtigt. Basis hierfür bilden neben den technischen Grundlagen und Hintergründe die Erfahrungen aus dem Projektalltag sowie die Diskussion mit den Teilnehmern.

Preis: € 1.890,-- netto

ComConsult IT-Sicherheits-Forum 2013, 23.09. - 24.09.13 in Euskirchen

Das ComConsult IT-Sicherheits-Forum 2013 konzentriert sich auf folgende Themenbereiche: Konsequenzen von SDN auf Sicherheitsinfrastrukturen, Sicherheit im Internet of Things, das vernetzte Fahrzeug, Cloud Sichere Nutzung und Aufbau von Clouds, Sicherheit in UCC, Gefährdungen bei IPv6, Sichere Identitäten in IP-Netzen, Network Access Control (NAC) in der Praxis Mandantenfähigkeit und Zonenkonzepte in RZ und Campus, Sicherer Betrieb von IT-Infrastrukturen: Authentisierung, Berechtigung, Protokollierung und Entkopplung der Kommunikation.

Preis: € 1.890,-- netto

Trouble Shooting in vernetzten Infrastrukturen, 24.09. - 27.09.13 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 30.09.13 in Düsseldorf

Immer mehr Unternehmen sehen sich derzeit damit konfrontiert, ihre Rechenzentrumsdienstleistungen über entfernte Standorte redundant anzubieten. Neben den entsprechenden Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Desaster Recovery Konzepte fordert auch die Kundenseite entsprechende Service Level Agreements zur Hochverfügbarkeit ihrer Dienste und Daten ein. In diesem Seminar werden die aktuellen Techniken vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
09.09. - 13.09.13 in Aachen
25.11. - 29.11.13 in Aachen
27.01. - 31.01.14 in Aachen
05.05. - 09.05.14 in Aachen

TCP/IP intensiv und kompakt
07.10. - 11.10.13 in Stuttgart
10.03. - 14.03.14 in Stuttgart
02.06. - 06.06.14 in Düsseldorf

Internetworking
14.10. - 18.10.13 in Aachen
07.04. - 11.04.14 in Aachen
23.06. - 27.06.14 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
24.09. - 27.09.13 in Aachen
25.02. - 28.02.14 in Aachen
20.05. - 23.05.14 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
05.11. - 08.11.13 in Aachen
18.03. - 21.03.14 in Aachen
24.06. - 27.06.14 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
16.09. - 18.09.13 in Berlin
09.12. - 11.12.13 in Köln
24.02. - 26.02.14 in Düsseldorf
05.05. - 07.05.14 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
07.10. - 09.10.13 in Stuttgart
10.03. - 12.03.14 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
04.11. - 05.11.13 in Bonn
17.03. - 18.03.14 in Bonn
30.06. - 01.07.14 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
30.09. - 01.10.13 in Düsseldorf
10.02. - 11.02.14 in Bonn

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research